Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/002623

International filing date: 31 January 2005 (31.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/540,161
Filing date: 29 January 2004 (29.01.2004)

Date of receipt at the International Bureau: 03 March 2005 (03.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1288820

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 24, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/540,161*
FILING DATE: *January 29, 2004*
RELATED PCT APPLICATION NUMBER: *PCT/US05/02623*

Certified by

Jon W. Dudas

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

PTO/SB/16(10-01)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

TO: Mail Stop Provisional Patent Application
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

Atty. Docket No.	CCCI 0122 PRV

INVENTOR(s)

FIRST NAME & MIDDLE INITIAL	LAST NAME	RESIDENCE (CITY & EITHER STATE OR FOREIGN COUNTRY)
Mark C.	Bell	Atlanta. GA
Paul D.	Brooks	Highlands Ranch. CO
Stuart C.	Cassell	Marietta. GA
Dallas S.	Clement	Atlanta. GA

X Additional inventors are being named on the 1 separately numbered sheets attached hereto.

TITLE OF THE INVENTION *(500 characters max.)*

NEXT GENERATION NETWORK ARCHITECTURE

DIRECT ALL CORRESPONDENCE TO:

CUSTOMER NO.

22045

ENCLOSED APPLICATION PARTS *(check all that apply)*

- X Specification - Number of Pages 61
- ___ Drawing(s) - Number of Sheets
- ___ Application data sheet. See 37 CFR 1.76.
- ___ CD(s). Number
- ___ Other: Specify

METHOD OF PAYMENT OF FILING FEES *(check one)*

	PROVISIONAL FILING FEE AMOUNT(S)	AMOUNT SUBMITTED OR TO BE CHARGED TO DEPOSIT ACCT.
___ Applicant claims small entity status. See 37 CFR 1.27.		
X A check or money order is enclosed to cover the Provisional Filing fees.	$160.00 (large) $ 80.00 (small)	$ 180.00
___ The Commissioner is hereby authorized to charge filing fees and credit Deposit Account Number:		

X Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

X The invention was not made by an agency of the United States Government or under a contract with an agency of the United States Government.

___ The invention was made by an agency of the U.S. Government or under a contract with an agency of the U.S. Government. The name of the agency is _____. and the contract number is _____.

X A return postcard is enclosed.

Respectfully submitted.

SIGNATURE Stephanie M Mansfield
REGISTRATION NO. 43,773

DATE January 29, 2004
TYPED or PRINTED NAME Stephanie M. Mansfield
TELEPHONE (248) 358-4400

CERTIFICATION UNDER 37 C.F.R. § 1.10

I hereby certify that this correspondence is being deposited with the United States Postal Service via Express Mail Label No. EV 375 982 875 US in an envelope addressed to: Mail Stop Provisional Patent Application. Commissioner for Patents.U.S. Patent & Trademark Office. P.O. Box 1450. Alexandria. VA 22313-1450 on:

January 29, 2004 (Date of Deposit)
Angelika Phillips (Name of Person Signing)
Angelika Phillips (Signature)

PTO/SB/16(10-01)
Approved for used through 10/31/2002. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

TO: Mail Stop Provisional Patent Application
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

INVENTOR(s) FIRST NAME & MIDDLE INITIAL	LAST NAME	RESIDENCE (CITY & EITHER STATE OR FOREIGN COUNTRY)
John	Collins	Greenwich, CT
Charles L.	Compton	Philadelphia, PA
John J.	Coppola	Cumming, GA
James W.	Fahrny	Pueblo, CO
Mark	Francisco	Clarksburg, NJ
Jason	Gaetke	Mullica Hill, NJ
Kenneth	Gould	Oakton, VA
Vincent T.	Groff	Dunwoody, GA
Harry	Hartley	Charlotte, NC
Michael T.	Hayashi	Aurora, CO
William	Helms	Longmont, CO
John G.	Hildebrand	Lawrenceville, GA
Stuart	Lipoff	Newton, MA
Fred	Pappalardo	Monroe, CT
James	Poder	North Wales, PA
Douglas J.	Semon	Denver, CO
Peter D.	Shapiro	Lexington, MA
Joseph W.	Weber	Louisville, CO
Richard	Woundy	North Reading, MA
Rouzbeh	Yassini	Nashua, NH
Jean	Pol Zundel	Berwyn, PA

CCCI 0122 PRV

Next Generation Network Architecture

Figures

Introduction

The present invention defines a next generation network architecture (NGNA) that will support the cable industry's expected market and business requirements, providing a reference model that cable operators and equipment vendors may elect to follow in making network and product investment decisions. The NGNA provides a cost-efficient platform with capacity and flexibility to support services such as on-demand video, high definition digital TV, home networks connecting a wide range of consumer-provided devices, and future multimedia services including IP voice and video telephony and multiplayer gaming.

The NGNA builds on on-going programs such as OpenCable™, PacketCable™, CableHome™ and DOCSIS®.[1]

Current Architecture

Cable TV systems currently employ hybrid-fiber-coax (HFC) networks that are inherently flexible to meet evolving requirements for capacity and for new service features. Cable TV operators have recently completed substantial rebuilding of their networks to increase their capacity generally to 750MHz and in some areas to more than 750MHz. The rebuilt cable networks can support new digital two-way services including new standard-definition program networks, new high-definition program services, on-demand video, high-speed data, and cable telephony.

These network investments have enabled cable operators to compete successfully today with digital DBS providers and telephone companies, to expand consumers' choices for cable-provided services, and to increase revenues from subscribers to multiple services.

However, the current architecture will need to evolve in order to meet future business and market requirements:

Next generation network requirements

Certain requirements have been taken into account in developing the next generation network, including the following:

Capacity

As cable operators add new services, demands for network capacity continue to increase. The next generation network needs to support expanding requirements for video program services, including high-definition services; on-demand video services; high speed data services involving enhanced downstream data rates and symmetrical upstream capacity; and interactive multimedia streaming services such as voice-over-IP (VoIP) telephony.

[1] CableLabs claims trademark protection for programs referred to herein including DOCSIS®, PacketCable™, CableHome™, OpenCable™ and OCAP™. Current versions of specifications for these programs are available at www.cablelabs.com .

Exploit existing assets

The next generation network should expand available capacity to meet anticipated service requirements within the current typical cable system bandwidth up to 750MHz for downstream transmissions. The next generation network also needs to continue to support multiple existing legacy assets, e.g., digital set-top boxes that use proprietary conditional access and out-of-band signaling. Support for legacy systems may be achieved by running the existing systems in parallel with next-generation systems. In this case, operational issues, including potential spectral exhaustion issues, must be addressed.

Secure rights management

Secure rights management of valuable content will encourage expanded participation by content providers in cable-provided services and support introduction of innovative new services and new business models. Content will need to be protected as it is networked among cable-managed devices in subscriber households.

Resource sharing

The next generation network needs to share network resources across services to enhance efficiency in the use of cable network assets. For example, QAM resources can be shared with dynamic provisioning by different services.

Managed subscriber devices

Home networks for video, data, and interactive multimedia services represent an important component of the next generation network. For example, media servers will be sharable across multiple home devices including subscriber video devices and Internet appliances. Further, to enable cost-effective configuration, provisioning and management of the widest variety of possible CPE devices in subscriber households, these devices will need to support automatic discovery and remote monitoring and control. Remote monitoring includes both the health of the device as well as the health and performance of the individual services that the CPE supports or transits. To accommodate potential new arrangements with third-party transaction or content providers, it will also be desirable for CPE to enable usage accounting.

Competitiveness

A key requirement for the next generation network is to enable cable operators to differentiate their services, or at minimum ensure competitive parity, in terms of features, functions and cost, versus offers from digital DBS providers, telephone companies and other competitors.

Flexibility

Cable operators need flexibility to rapidly provision and support new services with equipment, features, and pricing tailored to the disparate needs of the wide range of subscriber households. Such new services may involve different business models than those currently offered.

Operators also need flexibility for cross-service promotions, for example to be able to offer free movies for upgrading data service.

The next generation network is a platform for launching many new services and needs to be easily extensible to add such services without stranding earlier investments.

The next generation network also needs to accommodate new compression and transmission standards, for example allowing cost-efficient evolution from currently-deployed MPEG2 video compression to standards offering equivalent video quality at much lower bit rates.

Scalability

The next generation network should be capable of cost-efficient growth to support additional services, new subscribers and/or increased simultaneous usage of on-demand and interactive services.

The architecture also should be able to scale "down" to work cost-effectively in smaller systems.

Align with external technology

The next generation network should exploit the technologies that will most benefit from continued innovation and cost reductions. Examples include the continuing gains in digital signal processing, memory, and optical communications systems. Innovation and cost reductions are expected in particular for non-proprietary technologies that are subject to competitive market forces and that are the focus of R&D efforts from direct and indirect suppliers.

Encourage retail

The next generation network should expand consumers' choices of CPE, including retail purchase of consumer electronics, PCs, and other devices that could connect to cable networks directly or indirectly. Such devices should work seamlessly in providing cable services along with MSO-provided CPE, in accordance with agreements between the cable industry and consumer electronics manufacturers, and with FCC regulations.

Support disparate subscriber household environments

Subscriber households vary from those with minimal basic video services to those with a full set of digital video, data and interactive multimedia services. Many basic video subscribers who subscribe only to analog video are not equipped with a set-top box and receive analog video programs directly on cable-ready analog TV sets. Others subscribe to digital video services and have a digital set-top box supplied by their cable operator. Still others subscribe to digital video plus high-speed Internet access, possibly including home networking. Some households subscribe (or will subscribe) to video and data, plus interactive multimedia services such as cable

telephony (VoIP), multiplayer gaming, and IP-based video-telephony; plus other services yet to be introduced.

For subscribers with limited services, the primary NGNA objective is transparency and low cost as well as providing an opportunity to up-sell to other services. At the high end, where subscribers may have a mix of analog and SD/HD video, linear and on-demand premium services, DVR, and high-speed Internet access, the next generation network CPE will typically offer advanced features and may more often be acquired by subscribers at retail rather than through the cable operator.

Minimize operations burden

It is anticipated that in many cases the next generation architecture should reduce cable operators' operational cost and complexity.

Support authorized third-party use

Cable TV systems currently serve as channels for third-party content providers under distribution agreements with the cable operators. The next generation network's increased capacity and capabilities will expand cable operators' opportunities to partner with third-party content and transactions providers. It is important that the next generation network provide the means for cable operators to encourage and support authorized uses, including authorized third-party use, while protecting the cable network from unauthorized third-party uses that may disrupt, impede, or impair the authorized services offered to cable subscribers.

Performance criteria

The next generation network needs to satisfy quantitative performance criteria in terms of capacity, reliability and latency for the services or applications carried by the network.

Align with MSO financial objectives

The architecture and interfaces should be implemented in a cost-effective manner, based on commodity and/or specialized hardware and software as long as they are cost-effective.

Investments in next generation network equipment need to result in near-term financial benefits such as improved operating efficiencies and/or growth in profitable subscriber revenue.

Current cable networks should migrate cost-effectively to the next generation architecture. Architectures and technologies requiring a complex or discontinuous migration path must provide significant benefits that clearly outweigh the cost and complexity of migration. "Cost effective" migration implies avoiding stranding existing assets. It also implies that the types of investments -- fixed versus variable, integrated versus modular -- are aligned with the nature of the market opportunities and subscriber environments in which the investments will be made.

Next Generation Architecture

A reference architecture including key components and interfaces is described below.

The reference architecture is not intended to work at cross-purposes with regulatory requirements for the retail availability of navigation devices or for support of CableCARD-enabled devices. The reference architecture is intended to create additional opportunities for retail consumer electronics equipment that would work seamlessly in providing cable services along with MSO-provided CPE. Not every reference design described herein illustrates a slot for a CableCARD interface, but the expectation is that manufacturers can rely upon the NGNA conditional access system re-configurable security hardware element and/or include a CableCARD interface, and that either version could be available at retail.

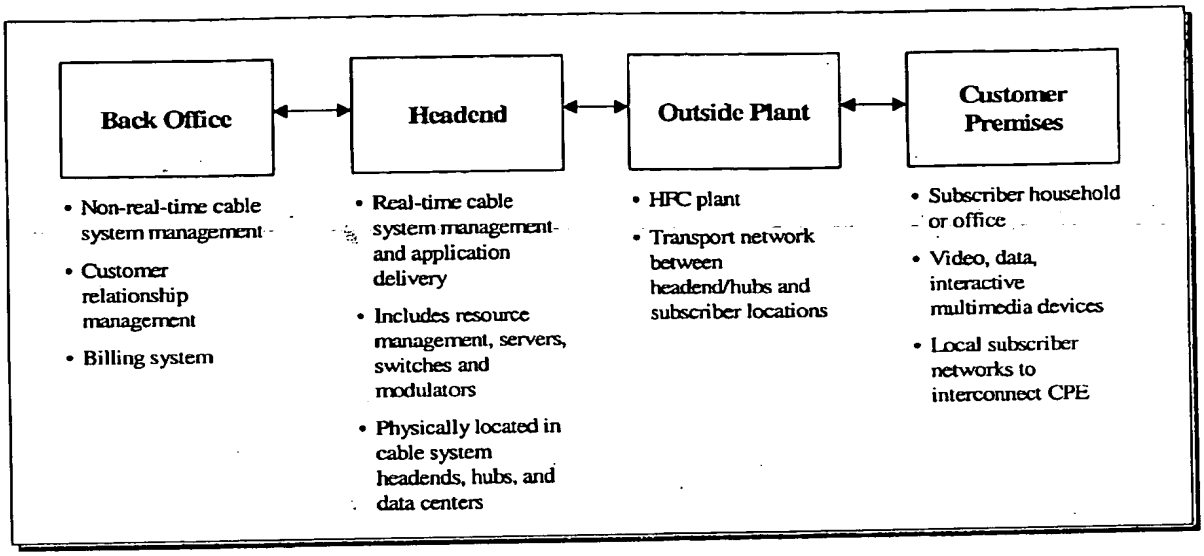
Reference Architecture Description

The reference NGNA is defined in terms of a set of network elements (NEs) and descriptions for how the NEs are used to meet specific requirements.

The NGNA will serve a wide range of subscriber environments from the most basic in which the only service is an analog video service, to a multi-service environment with digital video, data, and multimedia services. At the consumer premises, some NEs are primarily transitional devices so that basic subscribers can continue to receive their basic cable service in a largely transparent manner even though the network has evolved towards the NGNA. Other next generation NEs are intended for longer-term use to enhance user experience, enable revenue growth and/or cost savings, and are more likely to be available at retail.

Network elements operate within each of the major network segments comprising the back-office, head-end/servers, outside plant, and consumer premises equipment, as diagrammed in Figure 1.

Figure 1: Major Network Segments



This reference architecture describes network attributes in the head-end, outside plant and customer premises network segments, as well as the interfaces between each of these segments and between the head-end and the back office. It does not include the internal back-office architecture, the regional networks that interconnect cable head-ends, or national networks that interconnect cable operators' metro-area systems and regions and link to content providers. The back-office network segment is perceived as involving a distinct set of issues and opportunities that can be addressed separately from the real-time management and operations that characterize the network from the head-end to customer premises.

In addition, the regional and national data networking systems are excluded from this description based on the view that the current evolution of regional and national data networking systems already benefits from innovative, competitive market forces and will not represent a bottleneck to the NGNA objectives.

Next Generation Network Architecture Elements

Given the market, technology and regulatory trends that are evident today, it can be predicted that cable services will increasingly offer:

- more choice of programming services;
- more subscriber control, through on-demand selectivity of content, management of program viewing (including network DVR), self-installation of services;
- expanded availability of high definition programming;
- integrated interactive multimedia, data and video services;
- competitive offers versus DBS, telephone company, and high-speed Internet options;

- subscriber access from a variety of devices including consumer electronics equipment purchased at retail; and
- extensive home networking of a wide range of CPE devices supporting video, data, and multimedia services such as IP voice and video telephony, sharing of still photos, multiplayer gaming, and customer premises management.

To enable these features, the NGNA represents a major shift in cable system capabilities towards substantially expanded capacity for new services and on-demand platforms, greater openness to innovative new equipment suppliers and supply arrangements, cost-efficient integration of technologies and resources, and operational flexibility.

The NGNA is envisioned as an ***integrated multimedia architecture*** with the following key attributes:

- Provides non-limiting capacity for new services without requiring rebuilds of cable systems beyond 750MHz nor splitting of nodes beyond 500 HP/node. This is accomplished by enabling cable operators to make more efficient use of spectrum through such options as re-use of analog channels for digitally-compressed video services, advanced compression algorithms, integrated spectrum resource management at the head-end, and switched digital video.

- Separates network elements in the head-end to allow integrated resource management for increased network efficiency, with open interfaces to facilitate reconfiguration for future service offerings.

- Provides options to cable operators for broadcast and/or unicast video transport.

- All next generation CPE supports DOCSIS 2.0. This provides secure 2-way authenticated channels between the head-end and CPE. Such channels are used, for example, for renewable conditional access key management, remote management of CPE, downloadable firmware updates, and reconfiguration of encryption algorithms. Use of DOCSIS builds on mature, well-known, low cost technologies and contributes to overall production volume resulting in additional cost reduction of the DOCSIS equipment used in cable HSD and voice services.

- The NGNA reference model assumes all head-ends are upgraded to DOCSIS 1.1 and support DOCSIS Set-top Gateway (DSG), and enables cable operators to upgrade to DOCSIS 2.0 (or beyond) when appropriate.

- Conditional Access (CA) is implemented through internal hardware that can be remotely configured or renewed by software downloads to implement legacy CA and to support new proprietary or non-proprietary CA. This provides flexibility at lower cost than removable CA alone. It enables next generation network CPE to work on any NGNA compliant-cable system, portable and movable across cable systems operated by different MSOs nationwide, thereby expanding the CPE market for additional suppliers and for retail distribution channels. At the same time, cable networks will continue to support separable security devices.

- Enables secure, rights-managed sharing of content and features inside subscriber households through home networking of cable-managed subscriber data devices and subscriber video devices. In addition, low-end devices are enabled to deliver high-end features from connected high-end devices, thus providing more value to subscribers while limiting CPE investment.

- Supports transition to all-digital services while continuing economically to support over 100 million analog TVs and VCRs.

- Encompasses a wide range of subscriber devices that incorporate next generation network capabilities providing solutions for disparate subscriber household environments.

- CPE that support downloadable applications are equipped at minimum with OCAP 1.0 middleware.

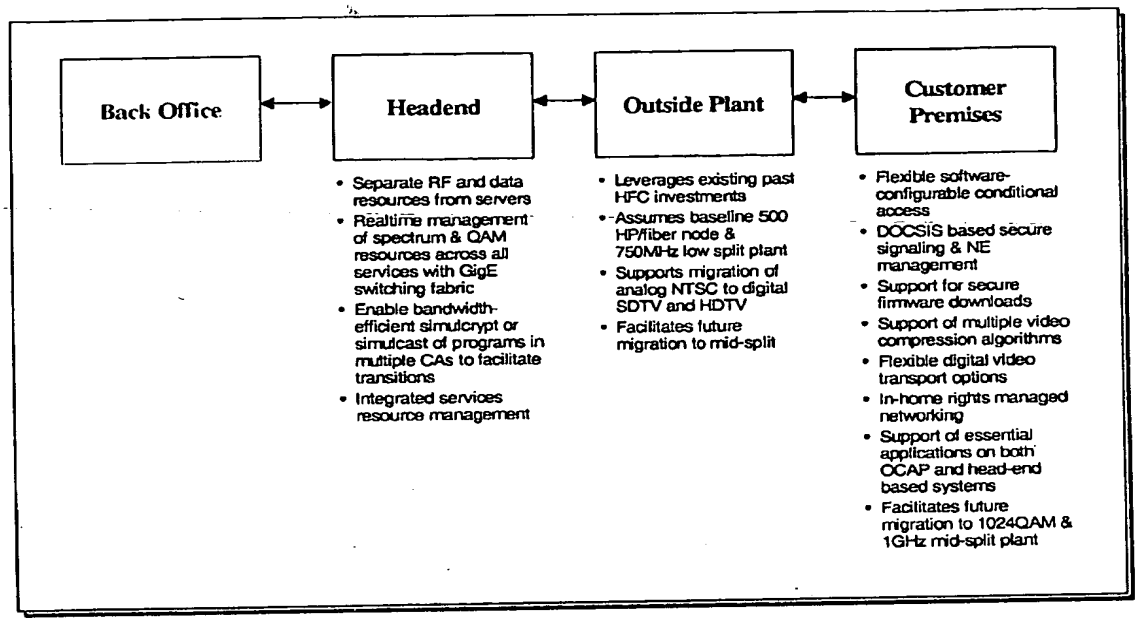
- Subscriber devices are pre-equipped to support future transmission and compression standards to enable cable operators to migrate to these standards without stranding prior CPE investments, whether these investments were made by operators or by consumers at retail.

- Rapid provisioning of new services is enabled by CPE auto-discovery, remote monitoring and remote management. Subscriber devices monitor the performance of the services that they support and provide both near-realtime alarms as well as summaries of exceptions.

- NGNA features are logically common across all in-home networked CPE, with associated subsystems in the head-end, which provides economies of scale for suppliers' R&D investments, reduced complexity in the head-end systems, and broader availability of these features to all classes of subscribers.

The following figure summarizes these attributes in terms of the network segments in which they are primarily implemented.

Figure 2: NGNA Aspects Across Network Segments



Video Services Architecture

The NGNA video services architecture assumes a common head-end and server environment compatible with a variety of NGNA subscriber premise network elements (NEs) that are connected to the in-home coax network. The NGNA video subsystems in the head-end are designed to provide a configurable and flexible CA, multi-service DOCSIS-based signaling, support for secure firmware/software downloads, support for MPEG-2 plus an advanced video compression algorithm, and flexible digital video transport options that are common to all next generation video CPE.

The NGNA will continue to support existing legacy CPE. The reference architecture also supports optional continued use of proprietary CA, with capabilities for secure software CA downloads to renew the CA key management and/or reconfigure the scrambling and key exchange algorithms.

The common aspects of the video services architecture include:

- **Conditional Access**: Support for both proprietary legacy CA and new CA.
- **Secure Firmware Downloads**: Device configuration and CA key exchange renewability.
- **Video Transport**: Support for multiple broadcast and unicast options over QAM, DOCSIS, or IP/QAM encapsulation.
- **Video Codecs**: Support for MPEG-2 and an advanced compression algorithm.
- **DOCSIS Signaling**: Employ DOCSIS throughout to facilitate remote management of devices.

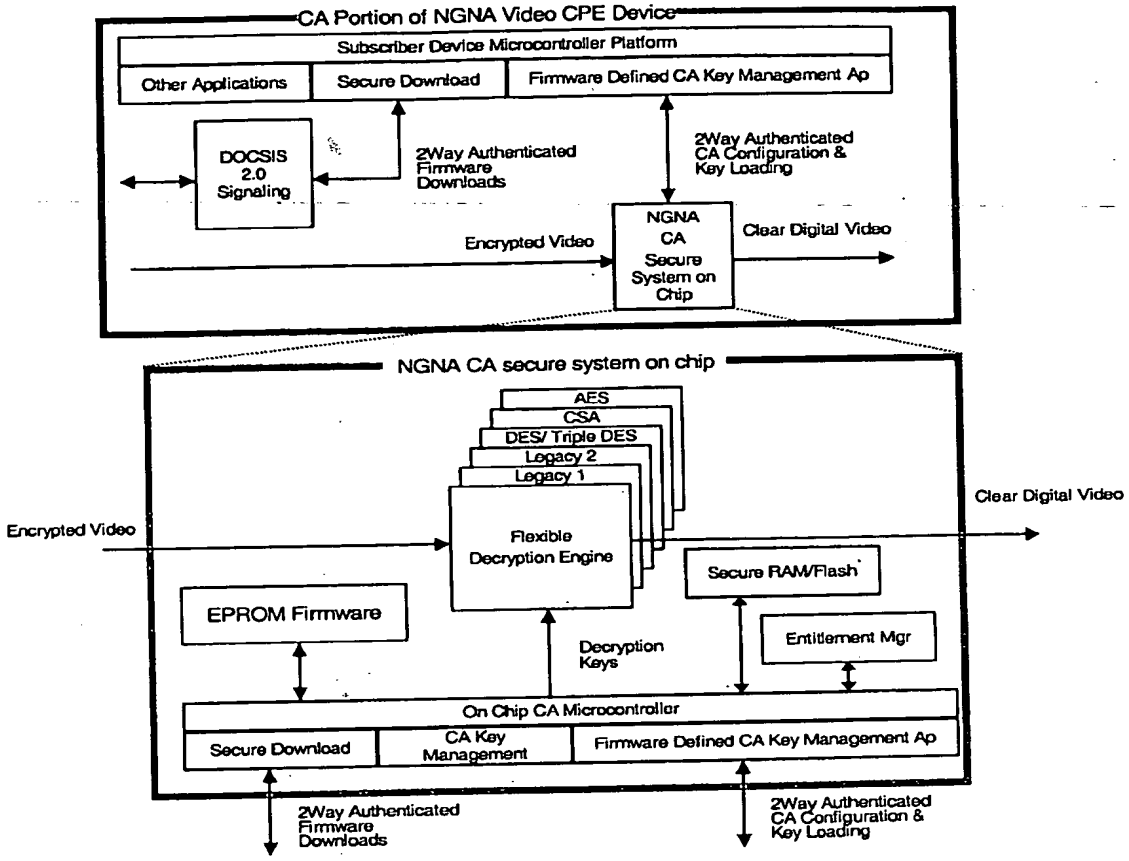
- **Video Client Software Environment**: Employ OCAP in all next generation network devices that support downloadable applications, plus provide flexibility to support applications through head-end based systems.
- **Secure Software Download**: Support for installing and upgrading software applications, drivers, kernels and OCAP implementations.

The NGNA encompasses subscriber video devices that might be provided by either the cable operator or sold at retail. The scope of this architecture therefore includes subscriber cable ready digital TV (DTVs) receivers and compliant video recording devices.

Conditional Access

The NGNA provides multiple conditional access (CA) options for the cable operator, allowing an MSO to support legacy proprietary CA as well as a new CA system. The new CA systems may be either proprietary or non-proprietary. Because the CA choice can be made anytime under control of a head-end command, a system equipped with NGNA subscriber devices can be migrated gracefully from one CA option to another. NGNA CA is compatible with CableCARDs. In the NGNA reference model, subscriber devices that have CableCARD interfaces will default to the NGNA CA if no CableCARD is installed. The reference model for the next generation CA model is shown in the following Figure.

Figure 3: NGNA CA Reference Model



The next generation CA model includes two subsystems: (1) content and key encryption/decryption, which is hardware-based but can be remotely re-configured; and (2) key exchange, which is software-based and thus re-definable by software download. In the CA reference model, content may be secured with either an open standard, non-proprietary CA system and/or a proprietary CA system (legacy or otherwise).

The "flexible decryption engine" in the CPE, as shown in the above Figure, is configurable to support multiple algorithms. It is flexible enough to allow configuration by remote command to be compatible with the encryption algorithms used by the CA system as well as the content protection system(s). Entitlement messages and control messages are encoded and distributed between out-of-band and in-band channels to the video CPE such that keys can be securely recovered by the CPE; this is referred to as the conditional access key exchange subsystem.

The reference model assumes that the secure aspects of the CA are protected by integration on a system on chip that includes a configurable decryption engine as well as on a chip micro-controller for key management. The assumption is that the secure

chip is protected using well-known hardware and software techniques to inhibit tampering or reverse engineering. In addition to the decryption engine, on board the secure chip is also the required micro-controller and firmware to support secure authenticated communications with the host next generation subscriber video CPE. These structures would therefore support cable operator management of two aspects of the CA:

- Remote reconfiguration of the decryption engine to support several pre-defined scrambling algorithms including commonly used legacy CA algorithms as well as new CA algorithms.

- Software-defined initial download and renewability of the CA key exchange mechanism.

To further inhibit tampering, all firmware images will be "code signed" and 2-way authenticated with head-end systems using well-known techniques to ensure integrity in the firmware.

Security Hardware Element
The NGNA Conditional Access System (NCAS) security hardware element supports the following standardized algorithms for transport stream encryption at the head-end and decryption at the CPE:

- Data Encryption Standard (DES) - Electronic Code Book (ECB), Cipher Block Chaining (CBC) and other modes for residual blocks [Federal Information Processing standard, FIPS 46-2]
- Triple DES – ECB, CBC, and other modes for residual blocks [FIPS 46-2]. This includes support for both two-key and triple-key encryption.
- Advanced Encryption Standard (AES) (Rijndael)
- DVB - Common Scrambling Algorithm (CSA)

The NCAS security hardware element is re-configurable to the various algorithms listed above. The NGNA system will support key sharing in the event that simulcrypt or multicrypt is required for legacy transition alternatives into the NGNA. In addition, the client device should possess the ability to operate in a simulcrypt or multicrypt environment.

The NCAS security hardware element is configurable ("renewable") and employs technologies to support the decryption of at least the following five types of secure transport streams:

1. DigiCipher II – as defined and licensed by Motorola.
2. PowerKey – as defined and licensed by Scientific-Atlanta.
3. Triple DES – supporting ECB and CBC at a minimum as well as two-key and three-key modes.
4. DVB-CSA – as defined in DVB.
5. AES – using a new standardized key architecture with standardized ECM, EMM, unit seed, and unit ID methodology.

Authentication

The hardware components of the NGNA CAS are capable of securely storing and performing digital signatures using various sizes (1024, 2048 and 4096-bit) of RSA keys in hardware registers. The next generation components are capable of securely generating digital signatures inside tamper resistant hardware without exposing the private keys or the processing needed to generate the hash, and encrypt. The next generation network is capable of digitally signing messages used for authentication and providing integrity using a secure SHA-1 hash.

Key Encryption Keys (KEK)

Next generation hardware is capable of securely storing Key Encryption Keys which could be in the form of symmetric or, preferably, asymmetric cryptography. The ability to use key pairs for transporting encrypted keys among CPE devices and to head-end devices is very desirable.

Unit Address (Public)

Each NCAS security hardware element used in a CPE device is uniquely identified with a completely unique ID. This ID is used to address each CPE device for receipt of the entitlements for that specific CPE device. In some implementations, a MAC address may be used for this ID.

Private Serialization

Each NCAS security hardware element used in a CPE device can contain a unique identifier known as a Private Seed ID. This Seed ID is used to generate the unique key to encrypt and decrypt the entitlements (EMM) for that specific CPE device. The CPE device is capable of changing the Seed ID to another unique value upon secure command from the head-end. The EMM encryption key is then generated using this new Seed ID as a component of the key.

Alternatively, each NCAS security hardware element could contain a Media Access Control (MAC) address as the ID and an RSA pair to validate the signature on the entitlements. The RSA key could also be used to decrypt the category key sent in the EMM.

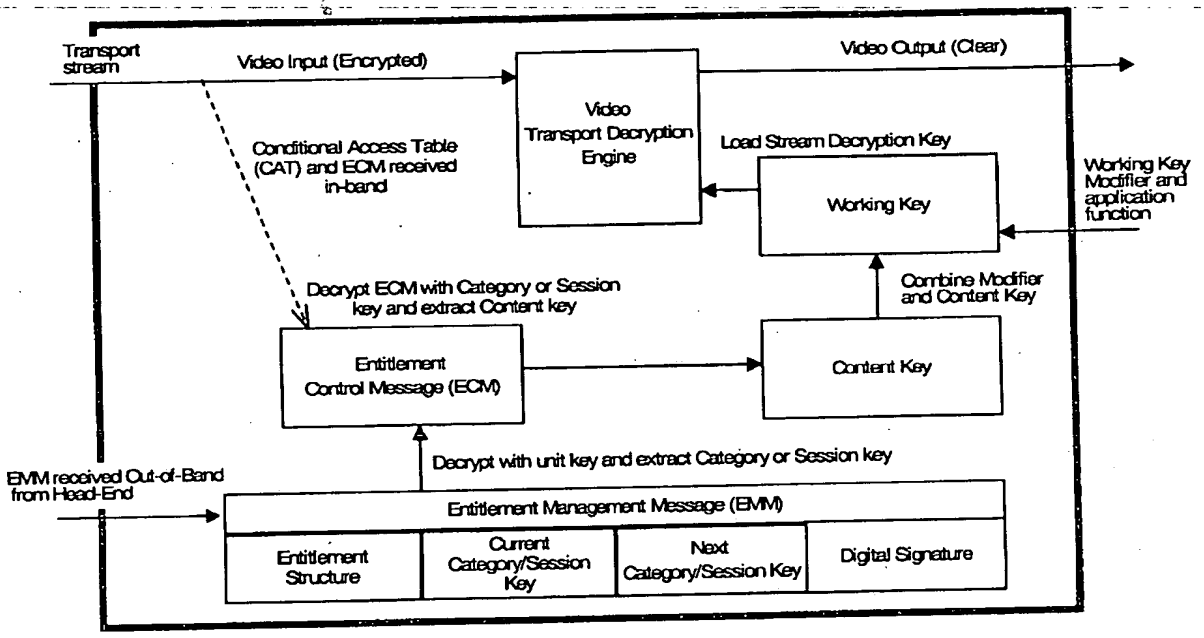
NCAS Tamper Resistance

The NCAS hardware performs all key generation processing, encryption, decryption, digital signature processing and key exchange algorithms inside tamper resistant hardware, which completely prevents the modification or unauthorized disclosure/analysis of the processing, Critical Security Parameters and private keys.

NCAS hardware is designed to meet FIPS-140 Level 2 security in most areas with some areas (hardware reconfiguration and firmware upgrades) requiring FIPS 140-2 Level 3 security. The NCAS hardware also employs the latest technologies (for example, power plane distribution and cell fragmentation) in tamper resistance to prevent electron microscope analysis and surface shaving attacks.

The key hierarchy includes (1) Unit or User Private key to the Distribution or Broadcast key, (2) Distribution or Broadcast key to the Authorization or Service key, and (3) Authorization or Service key to the Control Word or Content Key, as shown in the following Figure.

Figure 4: Key Hierarchy



NCAS Key Management

The NGNA CAS software and hardware is designed to employ new concepts and technologies in the area of key management while functioning with existing legacy systems using key sharing or re-configuration criteria. Decrypted keys extracted in the CPE from the video stream and ECM's and EMM's will be loaded directly into the decryption engines without passing over external interfaces including the transport decryptors.

Entitlement Control Messages (ECMs)

An ECM is an encrypted message that contains access criteria to various service tiers and a Control Word (CW). The Control Word is the seed key that is modified and used to decrypt the video stream and shall be able to be changed on a variable periodicity or in effect converted into a "working key." The ECM is decrypted and checked in the CPE against the access criteria in order to provide authorization. If authorization is granted, the CW will be released, converted to a working key and used to decrypt the content at the CPE device.

Entitlement Management Messages (EMMs)
Encrypted messages are created in the head-end and sent to the next generation CPE to authorize the CPE device for certain access criteria to content. The EMM contains the actual authorization data and shall be sent in a secure method to each CPE device. The EMM is addressed to a single CPE device and is uniquely encrypted so that only that device can decrypt the entitlements and validate them. The NCAS security hardware element supports DigiCipher II, PowerKey, NDS, Nagravision, and NCAS entitlement mechanisms and formats.

Software Renewability
Certain aspects of algorithms, key exchanges and cryptographic protocols are implemented in software or renewable firmware. Renewability in software is an important aspect of a strong security system and is preferably utilized in the next generation system. For cost reasons, it is desirable to use software renewability as a substitute for hardware renewability in as many situations as possible.

Hardware Renewability
Hardware renewability of the key management can be achieved in the form of a removable smart card. Full renewability of both key management and transport decryption can be achieved in several ways using removable hardware capable of supporting the bandwidth requirements of the transport stream. For NGNA devices that support a CableCARD interface, the insertion of a CableCARD allows full renewability. Alternatively, an expansion port such as USB2 could be used to host a new device that could be deployed for full renewability if device security were compromised.

Although software renewability is more cost effective and easier to implement operationally, some level of hardware renewability is preferred in NGNA CAS in the technology for key management and transport decryption. It is important to allow renewability consistent with the need to balance security against costs.

Secure Firmware Downloads
Each of the next generation video CPE devices is assumed to support three types of secure firmware downloads:

- General CPE control firmware that controls the user interface, device operation, and support for applications (e.g. VOD, EPG, OCAP);
- Internal CPE firmware that manages and communicates with the secure CA system on chip (SOC);
- Messages intended to be passed to the secure CA SOC which reconfigure the hardware engine and/or install CA key management firmware in the CA SOC.

As shown in Figure 3 above, the secure downloads are encoded for transmission to subscriber video CPE over a secure channel. All of the secure download signal paths require two-way authenticated exchanges and it is further assumed that physically accessible signals paths between blocks in Figure 3 are encrypted.

Copy Protection
If an NGNA device employs a CableCARD, the interface will implement renewability and configurability in compliance with SCTE-41. In addition to supporting the current SCTE-41 transport stream requirements, next generation Copy Protection CPE hardware elements is capable of decrypting the following three types of secure transport streams:

1. Copy Protection - DES (as defined in SCTE-41, with the additional option of using DES-CBC mode in addition to EBC mode).
2. Triple DES – supporting ECB and CBC at a minimum.
3. AES – using a new standardized key architecture with standardized ECM, EMM, Key Encryption Keys, and unit ID methodology.

Authorized Domain Security
The next generation security preferably supports an Authorized Service Domain (ASD) in a home network environment. This is primarily viewed as key management and the ability to store both symmetric keys for encryption/decryption and/or asymmetric key pairs for authentication. The next generation system preferably supports the ability to transport video and audio content to trusted display and recording devices in the home network. In-home network architecture, including the ASD concept, is described in detail below.

Video Transport
Digital video and audio streams are typically carried over MPEG-2 transport streams. Both Single Program Transport Stream (SPTS) and Multiple Program Transport Streams (MPTS) may be delivered at various segments of the system. MPEG-2 Program Specific Information (PSI) and ATSC/SCTE defined System Information (SI) are used at the transport layer.

Backbone
The backbone video transport (broadcast and on demand) is MPEG-2 transport over User Datagram Protocol (UDP)/IP carried over Gigabit Ethernet. Both SPTS and MPTS may be used. An example of SPTS is a Video On Demand stream at the streaming server's Gigabit Ethernet output. An example of MPTS is the multiplexed broadcast streams from a multiplexer.

Current industry practice is to encapsulate 7 MPEG-2 transport packets per UDP packet. Both constant bit rate (CBR) and variable bit rate (VBR) are supported.

The IP-based video transport is terminated at the edge of the head-end network element. In the NGNA reference architecture, the edge termination may be a QAM modulator or a CMTS to forward the IP traffic.

Edge to Subscriber Premises
The NGNA reference architecture includes three alternative means to carry MPEG-2 transport stream between the head-end edge (e.g., QAM or CMTS) and the subscriber premises:

- **Baseline: MPEG-2 Transport over QAM**
  Multiplexed MPEG-2 Multiple Program Transport Stream (MPTS) over QAM is the conventional approach used in today's digital cable system. In order to maintain backward compatibility, the digital subscriber video device (SVD), or next generation video CPE, is able to process MPEG-2 transport over QAM for both broadcast and on demand applications.

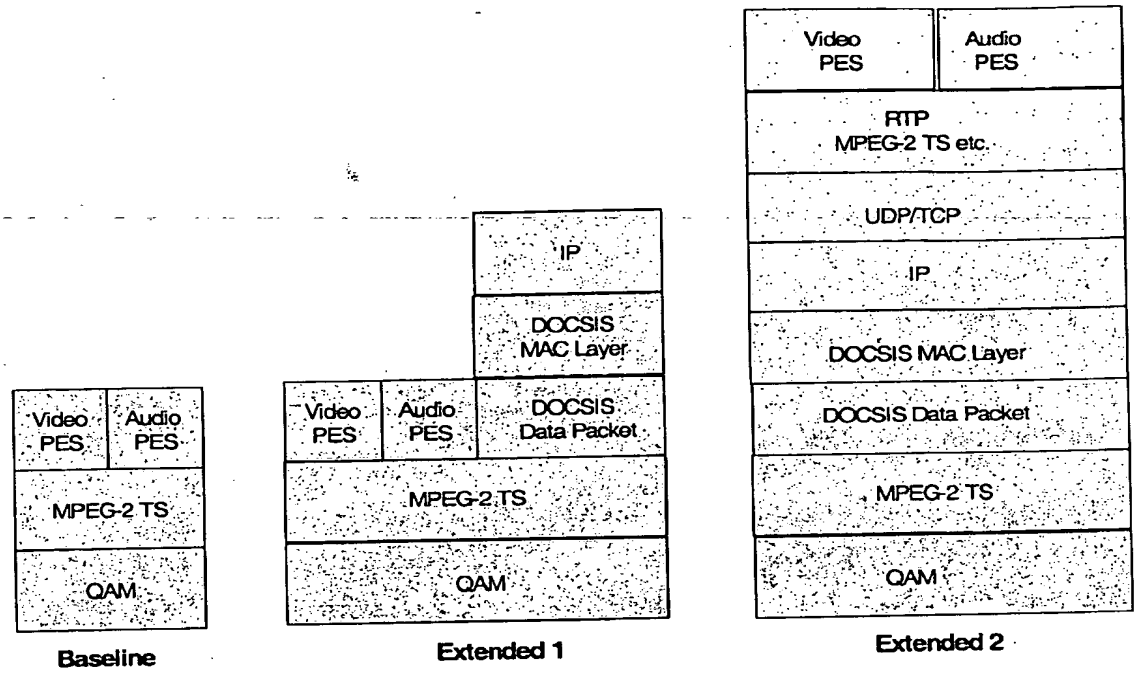
- **Extended 1: MPEG-2 Transport multiplexed with DOCSIS**
  In this approach, the MPEG-2 transport stream (DOCSIS downstream transmission convergence sublayer) is used to multiplex audio and video program information with DOCSIS data. The well-known PID 0x1FFE is used for MPEG-2 transport packets carrying the DOCSIS payload, and other PIDs are used for various video streams. In NGNA, this video transport approach can be used in addition to the baseline MPEG-2 transport over QAM approach to support advanced video based multimedia services that are integrated with data over cable services.

- **Extended 2: Video over IP/DOCSIS**
  In this approach, video is carried over IP and delivered over DOCSIS channels. This allows future services such as IP based streaming media to the digital set-top boxes.

  It is possible that video and audio streams can be carried over MPEG-2 transport stream and/or RTP or other protocols before it is sent over TCP or UDP packets.

  The subscriber terminal should support the MPEG-2 transport over QAM as baseline. In addition, it should be able to process the video transport over the other two extended methods.

Figure 5: Alternative Video Transport Approaches



Video Codec

The reference architecture assumes support for MPEG-2 and one additional advanced compression algorithm that can be remotely designated by the head-end. Several emerging techniques such as MPEG-4/Part 10 Advanced Video Coding (AVC), Microsoft Windows Media 9, and Real 10 have been widely discussed in the industry as options for deploying a codec that is more efficient than the current MPEG-2 codec. Utilization of an advanced codec needs to balance quality of the overall user experience, efficiency in the use of plant resources, availability, and cost.

Among the key specific factors are:

Compression Efficiency

- Overall compression efficiency compared with MPEG-2
- Example of technology enhancements to MPEG-2 may include:
  - Better motion estimation resolution
  - Multiple forward, backward, and bi-directional prediction modes
  - Better quantization and transform coding
  - Alternative entropy coding techniques
- Other advanced coding techniques that may be significantly different than the block based predictive coding could also be utilized.

Complexity

- Complexity of decoder (e.g. processing, memory usage and I/O etc.)
- Complexity of encoder (e.g. processing, memory etc.)

Flexibility

- Video resolution and scalability
- Latency for the encoding and decoding process (e.g. for live content)
- Flexibility for future encoding improvement
- Interoperability to enable content encoded by one supplier's product to be decoded by another supplier's product

Features

- Fast channel change
- High quality trick mode file generation
- Seamless splicing
- Error resilience
- Best effort or QoS based delivery

In addition to advanced video coding techniques, advanced audio coding schemes with significant improvement over the currently deployed Dolby AC-3 scheme could also be utilized.

Cost Evaluation

It is desired to implement the advanced codec in a cost effective way. This is particularly important for the decoder in a high volume, low cost environment. Silicon integration is certainly a key to drive down the cost. Other factors such as memory usage, I/O performance, as well as software/firmware are considered for the overall cost.

Product Implementation

There may be several ways to implement the advanced encoder and decoder. For example, they may be implemented in silicon with single or multiple remotely configurable chips, or in programmable DSP, or a combination of above. The tradeoffs between cost and flexibility are considered. In addition, there must be a mechanism in place to update the encoding algorithm once the system is deployed.

DOCSIS Signaling

The NGNA reference model includes multiple roles for DOCSIS including secure signaling for all CPE and alternative transport of video. For multimedia services, DOCSIS supports streaming media for which QoS is an important factor. DOCSIS transport and DOCSIS set-top gateway (DSG) protocols support secure software download and remote configuration management of CPE subsystems enabling:

- Configuration of the video decryption engine
- Downloadable key exchange aspects of the conditional access system (CA)
- Downloadable renewable firmware for basic control of the devices
- Remote configuration of the video decoder algorithm
- Downloadable applications designed to run on OCAP middleware

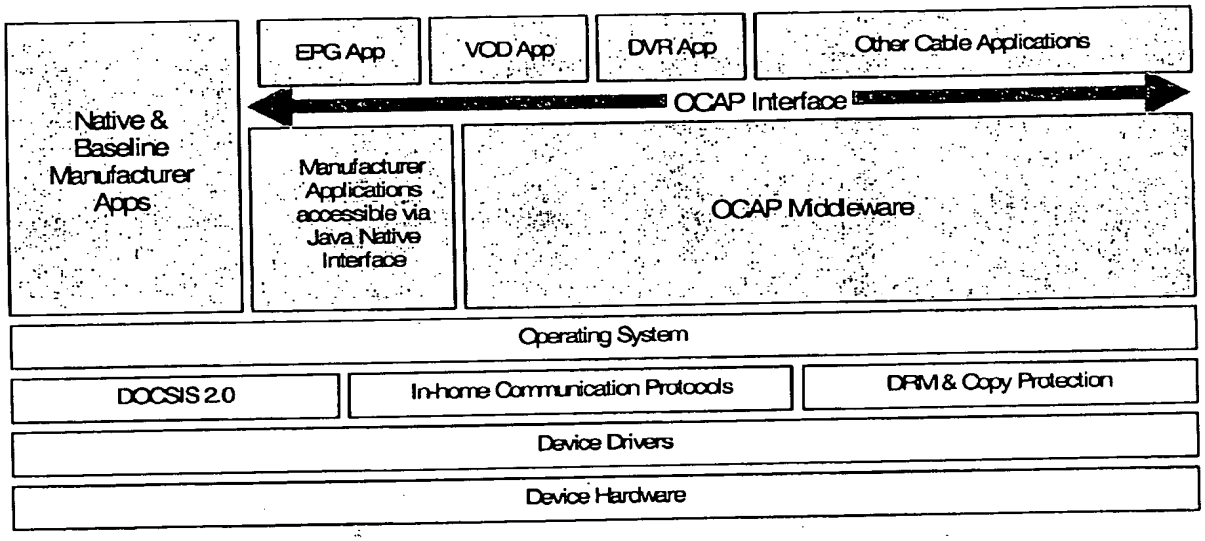
Important additional benefits of employing DOCSIS are its native features for remote management from customer support systems and operation support systems. Consistent with CableLabs' CableHome™ initiative, this capability allows all CPE to be visible from the head-end.

Video Client Software Environment
The NGNA reference model includes a minimum of OCAP 1.0 middleware in all video CPE that support downloadable applications. This provides a consistent environment for such applications that run on the OCAP middleware.

OCAP comprises a set of API's for the middleware component of a software solution. OCAP specifies a set of permission request files, a digitally-signed code image and a monitor application for various security and resource contention issues.

The following Figure describes the software architecture in the video CPE that include OCAP.

Figure 6: Video CPE Software Architecture



The reference model identifies two categories of native applications that the device manufacturer would preferably include in its products. Manufacturer's applications described as "native and baseline" have direct access to the operating system and bypass the OCAP layer to interface directly to host and user interface; for example, these might include giving the user the ability to select between cable-ready versus off-the-air broadcast mode of operation. The other category of manufacturer applications is designated as "accessible via Java Native Interface" (JNI). These applications are also supplied by the manufacturer and map through the OCAP middleware layer. The default for OCAP is to pass these applications through to the host and user interface; however, OCAP has the ability to modify the default or even to supplant the OEM application with a new application, for example, by one downloaded by an end-user on top of OCAP. An example of such default native applications might be up/down control of the sound volume on a DTV. Normally OCAP would allow the manufacturer's application to have control, but in the event of an emergency alert (EA), the MSO EA application running on top of OCAP could take over control of the sound volume.

Downloadable applications run in the OCAP middleware environment. Examples of applications that an MSO may choose to download would most likely include at least a small core set of essential applications: electronic program guide (EPG), video on demand (VOD), and other cable applications such as support for head-end rendered applications. With this last option, the visual display of the user output interface is created as a still video frame picture at the head-end for freeze frame display by the CPE, or alternatively this may be implemented as a unicast video stream if bandwidth allows and the user interface involves moving components. Support for the user input interface would consist of relaying user interaction with the remote control back to the head end to communicate a menu selection, or cursor selection, from the display.

There are expected to be differences between CPE devices in terms of applications and capabilities that are supported. For example, high-end devices will support some applications, such as DVR, that are not present on lower-end CPE. Transitional CPE devices, such as devices used to facilitate network analog-to-digital conversion, are not expected to include in-home networking protocols while more permanent CPE devices will support in-home networking.

Next generation client software is an important component in the overall system security architecture. Since system security for boot-time authentication, device drivers authentication and system kernel security is not covered in the OCAP specification, and since this creates risk of security compromise, it is important to specify the other security requirements for the complete next generation client software solution. The solution includes a trusted and non-modifiable boot loader that is the foundation of all software downloads and upgrades. It also includes the authentication of all software elements including OCAP implementation, system kernel, device drivers, OCAP applications and all other software at both boot time and during download. In addition, it includes trusted kernel technology which creates a trusted environment for task context switching.

Head-End Based Applications

The software environment should display applications and information for users in a flexible way. Designating OCAP in all the reference designs enables MSOs to customize the "look and feel" of each service. Some MSOs may choose to include a head-based application to provide flexibility to compose the user interface display at either the head-end or locally by the device-specific microcomputer.

A head-end solution would enable the rendering of the user interface and execution of the application to occur in the head-end, where components can be more easily added, replaced and upgraded.

In this mode, the CPE displays video (potentially stills) generated in the head-end, and transmits user interface actions (e.g., keys pressed on the remote) back to the head-end. In this way, servers in the head-end could run the application and UI, providing an extremely flexible way of adding almost arbitrary new applications to this parallel software environment.

The headend-based mechanism could provide a useful extension capability for the software environment.

Advanced User Interface
OCAP and head-end based applications can be employed together with other NGNA elements to provide advanced user interfaces to new services. Since the next generation network architecture supports a much richer variety of services as well as rapid service introduction, it is desirable to have intuitive user interfaces that are convenient and easy to learn to use.

Expanded hardware and software user interface concepts are desired that support next generation network objectives, in addition to baseline remote control keypads and/or keyboards. The scope of the user interface concepts includes:

- Advanced remote controls with new input devices such as touch pads, pointing devices, and software defined keypads;
- Remote controls, or other ancillary devices with screens additional to the main display screen that allow messages, web pages, navigation, help, or control information to be displayed to one person or multiple persons in the same room;
- Non-typical input/output devices such as force feedback on game controls, vibration devices keyed to program content, special effects generators that present 3 dimension sound effects, etc.

Multimedia Services Architecture

In the near future, it is anticipated that cable-provided interactive multimedia offerings will grow beyond traditional telephony to include, as representative examples: the sharing and display of still photos, high-quality, full-motion video telephony and conferencing, presence-enhancement for emerging communications media, applications-sharing and collaboration tools, and online-enabled multiplayer gaming. As such, the term *multimedia services* is employed herein to refer to IP telephony plus expanded multimedia offerings.

A small set of applications is currently defined in the multimedia services architecture, principally: high-speed data service and VoIP-based telephony. The high-speed data service is based upon technologies developed on the DOCSIS project at CableLabs, while the VoIP architecture has been specified under the PacketCable umbrella.

In addition to these core services, the next generation multimedia services architecture is positioned as an enabling platform for a rich suite of applications addressing a wide range of CPE devices. Potential multimedia service endpoints might include OCAP subscriber devices connected to the coax network, PCs sharing a DOCSIS high-speed data connection over the in-home data network, and personal wireless devices providing mobility and convenience functions within the home. A sampling of prospective multimedia applications hosted on these CPE follows:

- PC(s) on the in-home data network configured as media servers and accessed by subscriber video CPE on the in-home network (coax, wireless, HomePNA, HomePlug, CAT5 wiring, etc) for high-fidelity presentation of music, video, or still pictures.
- Gaming consoles interfacing with both video CPE and the home and access data networks facilitating participating in online multiplayer gaming sessions.

- Video telephony terminals and mobile, wireless communications devices receiving enhanced QoS-based network support while sharing infrastructure with other services within the home.
- Internet appliances that provide for telephone caller ID display, call logging, and message retrieval on subscriber video devices and PCs

The present invention also contemplates extensions to the cable network that will enable cable operators to partner and/or compete with wireless voice and data service providers, supporting wireless service offerings such as:

- Unified messaging services that integrate wireline with wireless universal numbering, voicemail, fax, follow-me voice, email, rich media messaging, virtual private networks, etc.
- IP mobility and roaming between cable modem services and public network WiFi hotspots.
- Deploying access points on outside plant to provide WiFi or other wireless technology coverage in public locations.

The next generation multimedia architecture enables QoS treatment for data traffic associated with specific multimedia services and involves functional components such as service provisioning and monitoring, digital rights management, and NAT-traversal.

Two broad segments of the network can be distinguished: the access network, defined as the HFC segment connecting the CMTS and cable modem (CM) elements, and the home network, broadly defined as the entire (physical-layer-agnostic) network topology behind the CM within the home.

NGNA incorporates mechanisms that primarily focus on the access segment and mechanisms that target the home network segment. In addition, the NGNA defines a bridge or gateway between the in-home coax network (typically an extension from the coax drip that connects to TVs and other video devices inside the home) and in-home data networks (typically subscriber-owned, often other than coax, that support PC-centric applications).

The present invention is not prescriptive about the nature of the in-home data network and assumes subscribers may elect any of a number of choices that are IP transparent and compatible with standard personal computer interfaces, (e.g., WiFi 802.11a/b/g, HomePlug, HomePNA, MoCA, and CAT5 wiring).

In addition to the access/home networking distinction, each of these segments themselves may be further decomposed and characterized according to the particular transport technologies used (e.g., MPEG-based QAM-modulation for traditional one-way video offerings, and DOCSIS MAC-layer transport for high-speed data products, both residing on the access portion of the network). For present purposes, we focus on the IP transport portion of the access network, and in particular the QoS capabilities that underlying DOCSIS technologies provide.

Overview of PacketCable Multimedia

The PacketCable Multimedia specification defines an application-agnostic technology framework for providing session-based QoS-enhanced network service over a DOCSIS 1.1 (or later) access segment. A fundamental prerequisite to the deployment of the PacketCable Multimedia framework is the availability of a DOCSIS 1.1 (or later) network, providing MAC-layer support for QoS. To facilitate the delivery of quality multimedia applications requiring QoS guarantees, the multimedia framework leverages these DOCSIS mechanisms and expands upon the architecture to support general-purpose QoS functionality based on mechanisms defined in the core PacketCable 1.x voice specifications. Several key network elements and interfaces have been identified and profiled within the PacketCable Multimedia specification (available at http://www.packetcable.com/specifications/multimedia.html).

PacketCable Multimedia and CableHome

While the distinction between access and home network segments is useful in describing the respective role that various networking technologies may play, the overall experience that a user will enjoy is dependent upon the end-to-end treatment that a service's network traffic receives. Consequently, it is important to address the boundary between network segments to ensure that appropriate coordination is provided in managing overall session quality.

Through the robust packet classification mechanisms introduced in DOCSIS 1.1 and carried on into PacketCable Multimedia, it is possible to identify and forward packets exiting the home network segment based on a number of distinguishing characteristics, including IP and MAC-layer originating and terminating addresses and ports, DiffServ/TOS marking and 802.1q VLAN tags.

Complementary QoS capabilities may or may not be provided on the home network segment, depending upon the layer-two technologies employed. CableHome 1.1, in particular, has adopted a packet-marking and priority queuing scheme based on 802.1q, as described in the home networking section herein.

PacketCable Multimedia and Regional Area Networks

Similar to the way in which DiffServ technologies are attractive on the home network segment, many Regional Area Networks (RANs) are also maturing to distinguish and route packets over divergent paths (with associated quality metrics) based upon packet marking. PacketCable Multimedia, in conjunction with DOCSIS, supports DiffServ strategies on the RAN by allowing the MSO to associate a particular DiffServ Code Point (DSCP) with each upstream service flow. All packets exiting this flow will be tagged with this DSCP before entering the RAN. Similarly, PacketCable Multimedia includes the capability to distinguish incoming downstream traffic received from the RAN and to place this traffic on an appropriate service flow based on DSCP markings (as well as conventional IP and MAC-layer originating and terminating address mechanisms).

Telemetry Services Architecture

Next generation networks should support telemetry and control applications such as home security, remote health monitoring, and energy management. These services can be deployed to any home passed by the cable infrastructure, regardless of a home's current subscription status. The network should support potentially large-scale deployments of endpoints that receive a constrained service set. To illustrate this further, consider the example of a remote meter reading service customized for use with a contracting utility. The meter would generate very low rate IP telemetry which could be carried over the broadband network from the source in the home (the electric meter) to the data aggregator (within the utilities' domain). The system will restrict data flows to that required for the application (in this case the electric meter and the data aggregation server) and prevent any unauthorized use of the network. The cable operator would ensure a monitored and robust connection to bring the meter data to the utility. The utility would deploy the equipment to every home in a geographic area.

Subscriber Premises Environment

In-Home Network Architecture

This section is about "in home networking" within and between the several networks that can exist within the home.

While many homes have one or more home networks today, they are generally not well integrated with the cable system and provide limited support for multimedia (e.g., best-effort delivery of low-quality video vs. guaranteed delivery of HD video.) Extension of cable operator-provided services and content onto home networks will enable a greater variety of devices to participate and provide new opportunities for novel services and business models.

The next generation network architecture includes a comprehensive in-home network architecture that supports the seamless transfer of traffic between devices on the cable outside plant (e.g., DOCSIS, MPEG-TS) and various home network segments/technologies. Examples of services and applications that the in-home networking architecture supports include:

- A low end subscriber video device (SVD) could access a high end SVD functioning as a digital video recorder (DVR) on the coax network for the purpose of viewing content stored on the hard drive of the high-end SVD. Thus, the low-end SVD would access the DVR application function of the high-end device without the cost of an additional hard drive and also provide a unified view of stored content at multiple locations in the home.

- A low-end SVD with limited memory and processing power could access OCAP supported applications running on a high-end SVD and obtain the application functionality as though the application were resident on the low-end SVD.

- A SVD on the coax in-home network could access video or multimedia media content resident on a personal computer located on the non-coax in-home network, or vice versa.

- Message traffic could be passed between the in-home coax and non-coax network to support applications such as display of caller ID on TV connected to an SVD or perhaps display of the e-mail inbox summary on a TV connected to an SVD.

The most demanding traffic on the in-home network in terms of bandwidth is likely to be high definition TV (HDTV) content (MPEG-2 based HDTV content can use up to 12 Mbps - 19Mbps of bandwidth for a single program). The next generation in-home network supports simultaneous real-time streaming of multiple HDTV channels within and between various in-home network segments and technologies.

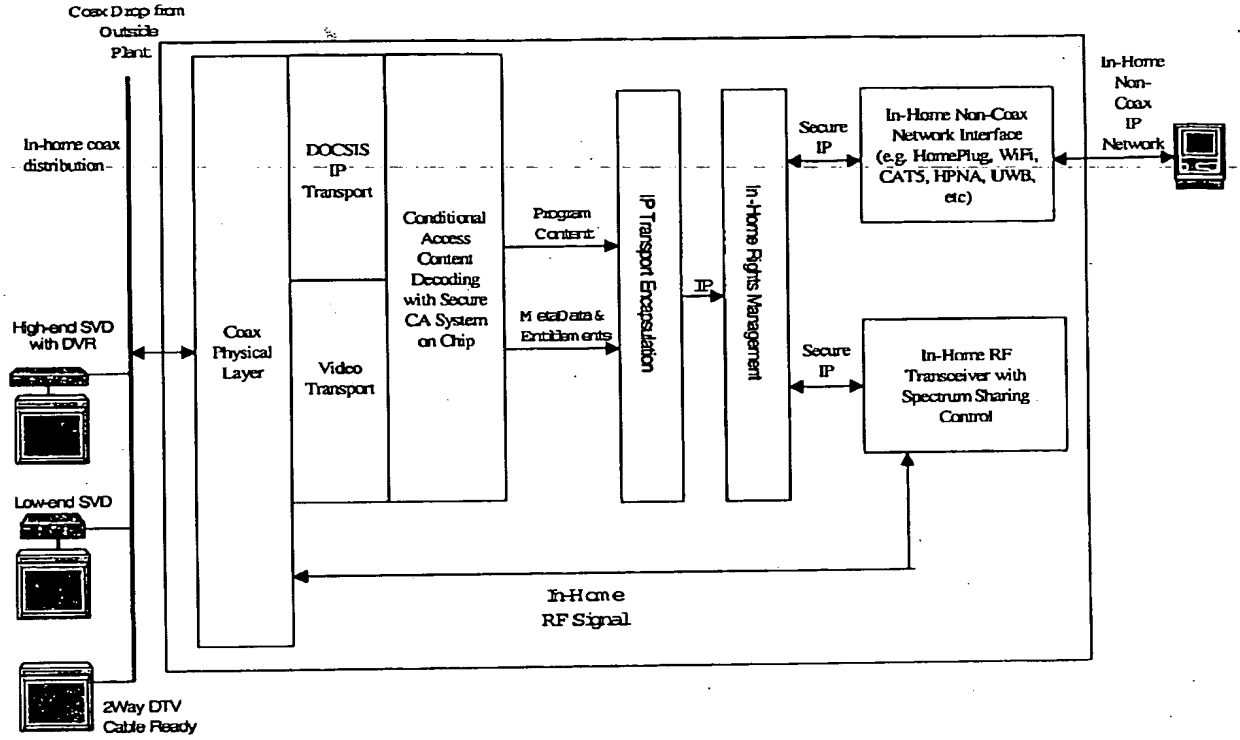
CableLabs' CableHome project has defined a home networking gateway element to bridge between the cable operator's DOCSIS network and the subscriber's in-home network(s). This gateway is designed to be provisioned and managed in a secure fashion, and additionally can prioritize packets passing between the DOCSIS and home network segments. The next generation in-home network architecture complements the foundation elements defined by the CableHome project with the considerations necessary to transport high quality content (e.g., content requiring rights management and stringent QoS enforcement) within and between each network, manage various LAN segments, and admit client devices to the network.

General Architecture Elements and Domains

A gateway element extends the functionality of CableHome Portal Services (PS). This gateway element adapts the in-home network segment(s) to the DOCSIS, and possibly MPEG-TS, network; this functionality includes transferring traffic among and between various in-home network segments(s) and technologies. The gateway may have many physical implementations, from embedded modems, to modem/NAT combinations, to implementations within an SVD. Herein we describe a high-end SVD as an example of such a gateway element.

As shown in the following Figure, the gateway provides the ability to support multiple transport technologies allowing traffic to move seamlessly around the premises in a transport-agnostic IP environment. The traffic on the in-home network may comprise various combinations of content, content control, navigation, and applications sharing to allow for interaction between data, video, and interactive multimedia (e.g. telephony) services.

Figure 7: Gateway Communications Architecture

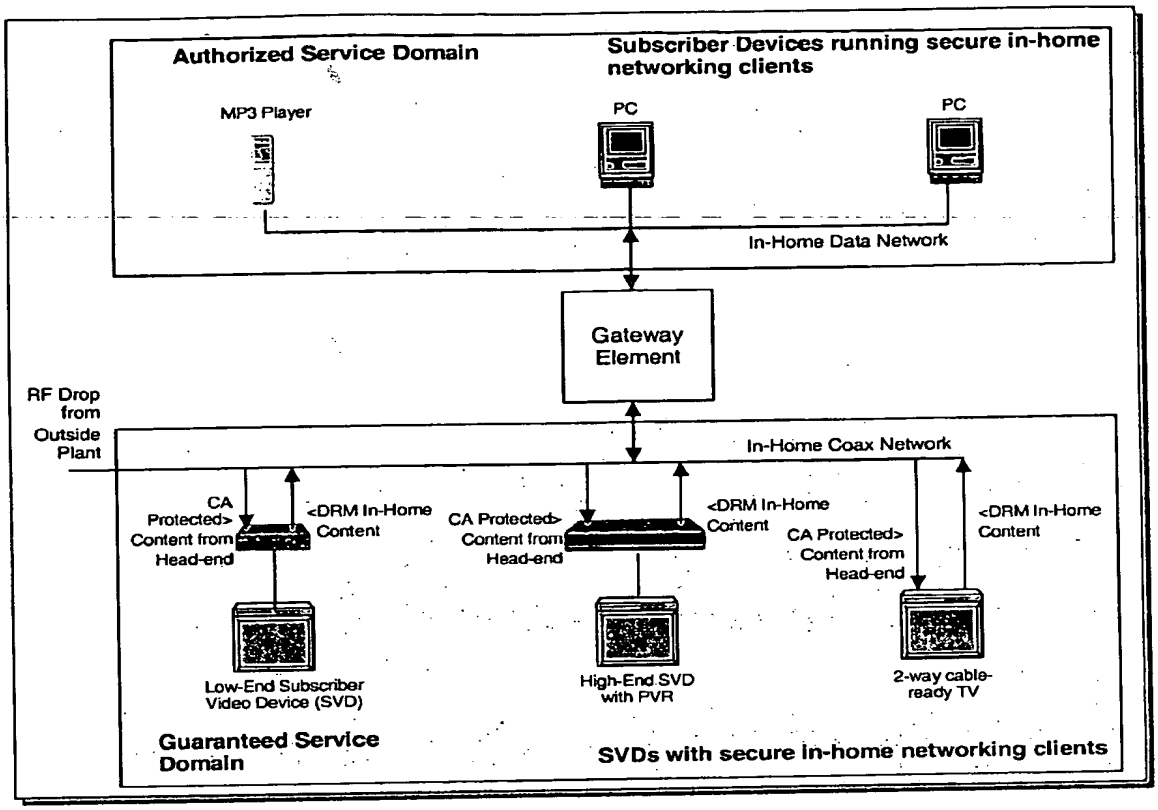


The various in-home network segments are unspecified at the media access control (MAC) and physical layer. Candidates for these layers include any known, or future, layers capable of high-speed internet protocol (IP) support. Examples of such layers include: Ethernet over CAT5, HomePlug power line carrier, Home PNA, MoCA, 802.11a/b/g/n. It is likely that many homes will utilize multiple home networking technologies to meet different needs within the home.

The various in-home network segments are assumed to be IP-based; in addition to providing continued support for high-speed data applications, IP provides a standards-based and ubiquitous interoperability layer across multiple network technologies and devices. The head-end has visibility of the QoS on the in-home network(s) and is able to prioritize traffic so as to maintain a desired level of QoS for cable-operator provided services and content. We believe that standard Internet protocols such as RTP and RSVP can be employed for this purpose.

As shown in the next Figure, within the communications architecture of the in-home network, there are functional domains that vary both by management of QoS and in terms of rights management (content protection).

Figure 8: In-Home Network Domains



If QoS can be maintained from the head-end to a client, it is considered to be part of the Guaranteed Service Domain (GSD). For this to happen, the client must support the appropriate QoS signaling, the home networking technology that the client is connected to must support QoS, and the home gateway must also support the appropriate QoS hooks. Hence, a given client may be in the GSD when connected to one network segment in the home and not in the GSD when connected to another. Similarly, a given segment is likely to have some clients that are in the GSD and some that are not, based on the level of QoS support in each client device and application.

Another domain exists that contains clients that are able to authenticate themselves and support content rights restrictions; this domain is called the Authorized Service Domain (ASD). This segment includes devices that comply with digital rights management.

Devices and physical layer segments not conforming to the requirements of the two defined domains may still be discovered and participate in services that do not require content protection or guaranteed quality of service, respectively. In addition, if NGNA home network management is unavailable, NGNA-compliant CPE devices should be designed to continue to operate, although possibly at a reduced level. Programmable devices may be conforming when running certain applications, and

non-conforming when running other applications. The GSD and ASD domains are independent; a device can belong to neither, one or the other, or both.

The NGNA structure of the present invention anticipates running compatible secure clients on the PCs so that rights managed content can be exchanged between SVDs and PCs. An example of an application might be to watch on a PC video from a DVR housed in an SVD. Alternatively, a PC could take on the role of a video or music server allowing for SVD access to the PC content. For example, a PC could serve as an advanced home answering machine or caller ID information could be displayed on a TV.

Use of the Coax for In-Home Networking

The coaxial cable itself is an attractive physical layer for in-home networks. It is generally present in many rooms in the house, is almost always present near televisions and other high-quality video displays, and has ample bandwidth to support a myriad of bandwidth-hungry services.

An important issue in using the coax for in-home communications is ensuring that in-home network signals do not interfere with current or future services being offered through the coaxial cable from the cable company. In addition to frustrating the customer by preventing access to cable services, such interference could affect other cable subscribers on the same cable network segment/node.

For this reason, any in-home coax physical layer must respect and be compatible with the outside plant physical layer in terms of upstream and downstream spectrum, FCC Part 15 regulations, and with signal levels within the dynamic range of the plant; this can be accomplished via interaction with the head-end to ensure compatible use of spectrum (preferred) or through isolation of the home coax segment from the outside cable plant. In the latter instance, such isolation may interfere with delivery of future cable services and also generally requires installation of an isolating element, such as a filter, near the point of entry to the home, which can be inconvenient. Also defined herein is an NIU network element that re-maps the outside plant spectrum to a new location within the in-home coax network that the in-home physical layer must also respect.

The NGNA reference design assumes that the in-home coax physical layer operating parameters are both visible to, and under control of, head-end systems. The reference design assumes that the head-end provisions the in-home physical layer with these operating parameters, e.g. upper and lower spectrum boundaries, and that once provisioned the in-home coax physical layers operates within the limits defined by the head-end.

The NGNA reference design assumes that the in-home physical layer and outside plant layer co-exist to a first order by non-overlapping spectrum assignments. However, it is contemplated that co-existence within the same frequency spectrum could be allowed by means such as time multiplexing or compatible modulation schemes such as wideband spread spectrum. .

With regard to the in-home physical layer, the MAC layer must mediate traffic between devices on the in-home coax network. The NGNA reference design assumes

that all devices on the in-home coax network are peer devices and that once these devices are provisioned by the head-end, they can share the in-home coax physical without any centralized management. The NGNA reference design assumes a MAC layer protocol that operates in a peer-to-peer distributed fashion to prioritize traffic so as to maximize the user experience. For example, a protocol should be capable of assigning higher priority access to streaming video traffic between devices on the in-home coax network than to delay-insensitive data traffic.

Content Sources and Clients

The in-home network architecture is specified to aid the seamless interoperability of content sources and clients. Content stores (i.e. music, photo and video libraries) that exist on networked clients may be discovered, cataloged, and streamed to other devices on the home network, and even optionally offered to authorized devices outside of the home network.

The in-home network architecture enables a convenient, unencumbered home network platform for the consumer while maintaining the integrity of protected (restricted) content within the Authorized Service Domain (ASD). Several assumptions are embedded within this framework:

- All content transport within the home is via IP (Internet Protocol);
- The network architecture transports many different types of media, including video, audio, "stills" (e.g. JPEGs) and data;
- The network architecture provides simultaneous support for MSO-supplied protected content and services, alternate-source protected content (e.g. a third-party music DRM solution), and non-protected content (regardless of source).

While there may be several embodiments of in-home network architectures that achieve the desired goals, a number of key technical points should be considered:

- Only authorized (i.e. certified) devices may be part of the ASD.
- The architecture must support transmission and storage of both MSO delivered content and non-MSO delivered content.
- MSO delivered protected content may be stored and consumed within the ASD.
- MSO delivered protected content may only exit the ASD through approved outputs.
- Protected and non-MSO delivered content may be consumed and stored within the ASD.
- Unprotected and non-MSO delivered content may freely exit the ASD for consumption on a non-trusted device if the device follows the FCC's Broadcast-Flag rules for screened and unmarked content.
- If the communication link with the cable network is disrupted, the in-home network architecture should still function for up to a certain length of time, with the time limit set by the cable operator.

In-Home Rights Management

The NGNA includes transitional video CPE within the Guaranteed Service Domain (GSD) to allow subscribers to continue to use legacy devices with maximum possible transparency. Both the transitional and more permanent CPE and SVDs share common CA and Out-of-Band (OOB) signaling. In addition, the SVDs support

rights-managed rich peer-to-peer in-home networking support between SVDs. A Gateway Element bridges between the GSD and the Authorized Service Domain (ASD) to enrich the in-home networking possibilities.

Content is delivered to each SVD within the Guaranteed Service Domain using the head-end managed CA as previously described. Each SVD includes peer-to-peer protocol support with copy protection provided by in-home networking digital rights management (DRM). The NGNA assumes that each device includes secure clients that can mutually authenticate to each other using digital signatures or a standardized key exchange technology. It is desirable for this authentication mechanism to be renewable by secure software download from some source device or server.

In the NGNA in-home structure, any SVD on the network has access to the features and content on any other device on either the GSD or ASD networks. The Rights Management System (RMS) should be capable of supporting multiple video streams for recording, real-time viewing and multiple viewing sessions.

Digital Content Security
The standardized algorithms for content encryption at the Rights Management System server and decryption at the end device on the home network are defined above.

Entitlements and License Management
The NGNA RMS is capable of translating entitlements and copy protection states and transporting these rights throughout the in-home network. The NGNA RMS is designed to employ new concepts and technologies in the area of key management while ideally functioning with existing legacy systems using key sharing or re-configuration criteria. Keys and Entitlements may be translated from the video stream Copy Control Information (CCI), ECM's, and EMM's to be loaded directly into the decryption engines without exposure in the content decryption engine on the home network device.

In the NGNA in-home rights management system, an XML-based Rights file that contains access criteria to various service tiers and a content decryption key are typically signed and encrypted. The content key is the key used to decrypt the content and may need to be changed on a variable periodicity. The entitlements and copy protection restrictions are decrypted and checked in the CPE against the customer access criteria in order to provide authorization. If authorization is granted, the content key is issued and used to decrypt the content at the CPE device on the home network.

RMS Tamper Resistance
In the NGNA in-home RMS, the RMS performs all key generation processing, encryption, decryption, digital signature processing and key exchange algorithms inside tamper resistant hardware/software, which would completely prevent the modification or unauthorized disclosure/analysis of the processing, Critical Security Parameters and private keys. The RMS should be compliant with requirements cited above in NCAS Tamper Resistance. The RMS hardware should also employ the latest technologies (for example, device power countermeasure distribution and cell fragmentation of keys and secrets) in tamper resistance to prevent various types of common hacker and reverse engineering attacks.

Applications Performance Management

As MSOs offer increasingly sophisticated, interactive services there will be an increased desire to monitor the experience of subscribing end-users for each application, in addition to traditional infrastructure and plant surveillance. Such monitoring, which will occur remotely at the operator's head-end or other network operations center (NOC), will apply to technical performance and will not provide any information for non-technical purposes that may have privacy implications.

Desirable features of this performance monitoring layer include:

- CPE will have the ability to monitor and collect performance and trouble data while offline. This allows for trouble data to be accumulated during periods when connectivity may fail and also distinguishes between an offline device (powered off) and one that is simply unable to connect. It also provides for better scalability than a centralized approach.

- Thresholds set to detect critical performance issues and send alarms to a NOC. This requires a facility to be implemented that produces SNMP "traps" or similar alarms.

- Thresholds set to detect minor performance issues and send periodic summary reports to a NOC (on the order of once/day).

- Alarms to uniquely identify the device/user.

- The ability to embed or download a performance monitoring application (PMA) for each user application (e.g. iTV, program guide, pay per view, web surfing, email access, etc). A PMA would be downloaded based on a class of the application to monitor.

- The ability for the PMA to register for details regarding flows of traffic, and to be delivered messages indicating timestamps and protocol headers (exact fields are a function of the class of application/protocol). Timestamps should be accurate to within 1/100 of a second. Flows should be based minimally on IP port number and/or destination IP address.

Advanced Digital Advertising

Advertising on cable is in the midst of a transition from analog to digital ad insertion. The NGNA will support this transition and a wide variety of advanced advertising models.

While cable's current ad insertion mechanisms are focused on linear broadcast content, it is important to develop new advertising models and technologies to extend the advertising model to include interactive content (including non-TV content) as well as non-linear video content (e.g., VoD, Network DVR.)

The NGNA will support advanced advertising models such as:

- Digital into Digital Advertising
- Targeted Advertising
- Interactive Advertising
- DVR Advertising
  - Showcase advertising – downloading longer form content directly to the DVR
  - Replacement advertising
  - Network DVR advertising
- VOD Advertising
  - On existing content
  - Local VOD ad insertion
  - VOD publishing for an advertiser

Supporting advanced advertising will involve the following:

- User Interface Navigation
- SVD data for marketing, affidavit and invoicing, while respecting privacy policies
- Capabilities and information extended to program providers

Methods to protect privacy of audience measurements build on current practices that include aggregating and anonymizing SVD change of state data; and protecting the uploaded data from being directly associated with a MAC address (for example, by a transcoding of the MAC address to another identifier). Such techniques also facilitate the sending of targeted ads to very granular demographics while protecting the identities of the recipients.

CPE Network Segment

This section describes NGNA-compliant CPE network devices. Each device is described in terms of features, functions, performance, technologies, hardware, IP rights, external interfaces, and target costs.

Overview

The CPE network segment involves significant opportunities and challenges vis-à-vis consumer electronics manufacturers, CE retailers, and FCC regulations, and the largest overall investment and inertia to change given the large number of devices. The following chart summarizes key features and attributes of CPE devices for which reference models are described herein.

Network Element	CA	In-home networking	DVR	OCAP	2-Way Apps Support	CableCARD slot	Transition device	Target cost to MSO
ODA- full function	Y			Y	Y		Y	<$50
ODA – all-DOCSIS	Y			Y	Y		Y	<$35
Video NIU	Y						Y	<$150
SVD – low end	Y	Y		Y	Y			<$150
SVD – high end	Y	Y	Y	Y	Y	Y		<$250
SVD – 2-way TV	Y	Y		Y	Y	Y		NA

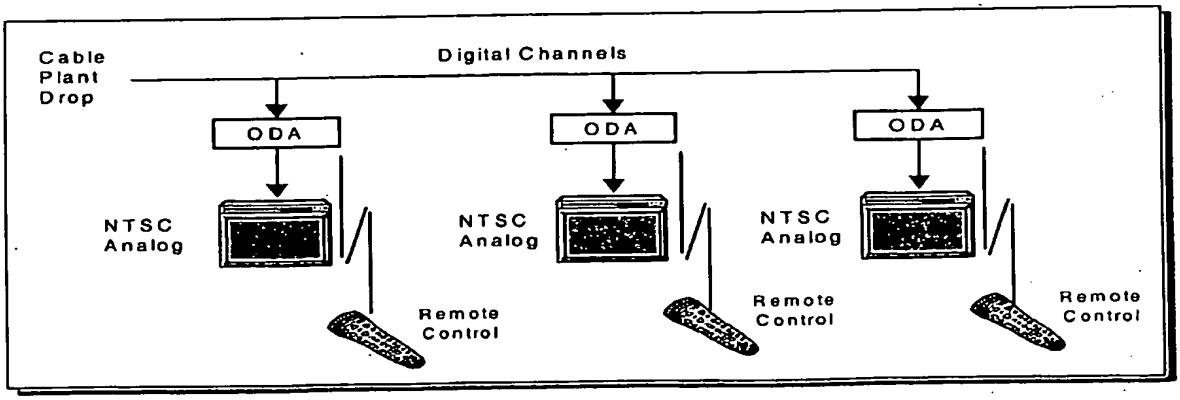
Outlet Digital Adapter (ODA)

ODA Deployment

Given the assumed limit of available downstream bandwidth on the outside plant at 750MHz, next generation network capacity requirements to support new services may require cable operators to reclaim bandwidth currently used for analog video services. Some or all analog services currently transmitted between 54MHz – 550MHz would be compressed as digital channels. As a result, these services would occupy a small fraction of their currently-used capacity, freeing the rest of the current analog spectrum for other services.

A large portion of subscriber households fall into the "analog video" category. They subscribe only to basic cable analog service, have analog TV devices, and do not use set-top boxes. Even "digital service" video subscribers often have one or more analog TV devices that receive only analog cable channels. To continue to serve these subscribers without imposing on them a set-top box that they may not want, one solution is to install an Outlet Digital Adapter (ODA) at each of these subscribers' analog cable outlets to convert the formerly-analog digital channels back to analog for continued direct reception on the subscribers' TV devices:

Figure 9: Example of ODA deployment



The next generation network architecture may include multiple possible ODA options:

- Full function 2-way ODA
- All-DOCSIS 2-way ODA

ODAs are transition devices that allow subscribers who have cable-ready analog TVs and other analog devices (e.g. VCRs) to continue to receive their existing services in a manner that is as transparent as possible even though the formerly analog channels will have been re-assigned to carry digitally compressed signals. Key considerations for ODAs are (1) cost, and (2) transparency for subscribers who prefer not having a set-top box.

Each of the ODA alternatives offers common next generation network architecture features:

- Includes means to decrypt program content and a remotely configurable conditional access system.
- 2-way capable in order to support several NGNA objectives:
  - — Reduced operating costs by giving MSO customer service and maintenance staff visibility of the subscriber equipment status;
  - — Allow for implementation of switched digital broadcast should an MSO elect to use this technology to use available spectrum more efficiently;
  - — Improve overall security against theft of service by allowing for downloading new firmware for conditional access and other firmware updates;
  - — Support on-demand applications.
- Includes DOCSIS 2.0 to leverage the manufacturing scale economies of DOCSIS integrated circuits and also to leverage the intrinsic capabilities of DOCSIS 2.0 with BPI+ to provide a 2-way secure authenticated channel between the head-end and the subscriber premises.
- Provided with a dual-mode video codec that supports existing MPEG-2 ATSC compatible compression and also a future advanced video codec that will facilitate future expansion of the video program bandwidth by at least 2X.
- Includes a companion universal remote control that can be configured by the subscriber to operate an existing TV and/or VCR.
- Designed to facilitate self-installation with input/output RF F-connector and plug in to AC mains for power. There is an on-screen display generator to show the channel number. To facilitate self installation, the display generator provides for on-screen install prompts to the subscriber such as: on-screen help of how to install and use, telephone number to call for help, cable plant RF signal level go/no-go indication, etc. The remote control includes a help button to activate the on-screen help messages.
- Supports applications capable of running on OCAP.

Also contemplated are possible variations on these CPE reference models that are not explicitly described herein and that may have significant cost implications. For example, an ODA may be designed solely to convert digitized channels back to analog for continued reception on subscribers' TV devices, without also providing support for applications such as VOD or EPG. Another ODA variant may be a transitional device that supports native applications such as EPG and VOD. In one

variant, this device would not support OCAP applications and would be purchased only by cable operators. For this device, cable operators would arrange for applications support in negotiations with the equipment suppliers. Another variant, depending on manufacturer interest, might include OCAP and a CableCARD slot and would be available for sale to subscribers at retail. These ODA variants are summarized in the following chart.

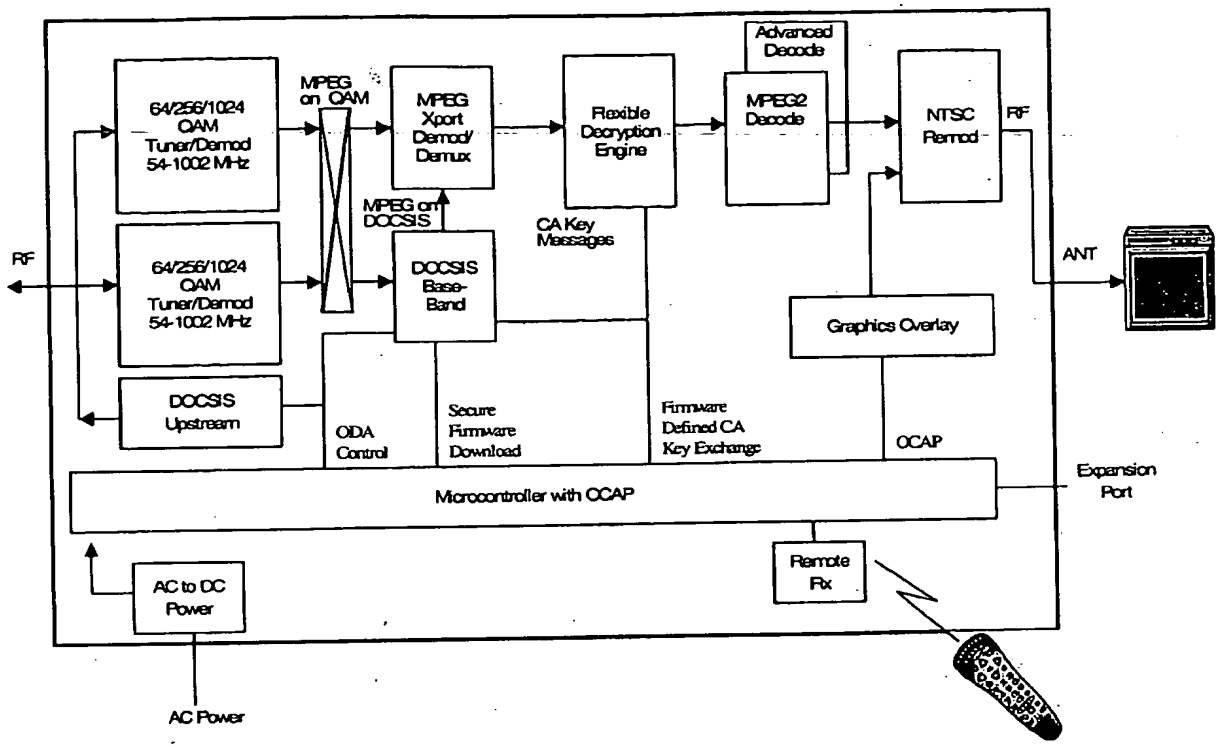
ODA	OCAP	Native Applications	Available at retail
RFI models	Y	All OCAP	Y
ODA Variant – No Apps	N	None	Y
ODA Variant – Native Apps	N	EPG, VOD	N
ODA Variant – CableCARD slot	Y	All OCAP	Y

Full Function 2-Way ODA

Except for a new remote control, the full-function ODA is largely transparent to basic video subscribers. The services remain the same, and the small ODA device is most likely placed behind the TV set.

In addition to allowing more efficient use of cable spectrum, the addressable two-way capability may also assist in promoting self-installation of the ODA devices, because it will enable operators to provide incentives such as free on-demand content and it will provide information to CSRs who may be called upon to help subscribers complete installation tasks.

Figure 10: Full Function 2-Way ODA Hardware Architecture



Key next generation features of full function 2-way ODA

- The reference architecture supports either an MPEG transport stream over QAM or via the DOCSIS channel. Furthermore the MPEG video over DOCSIS can be either broadcast video encoded in the downstream DOCSIS MPEG convergence sublayer, or alternatively can be unicast as MPEG over IP.

Functions

In addition to features described for ODAs in general, the following applies specifically to the full function ODA:

- Dual tuners which support access to digital broadcast unencrypted or encrypted services can apply digital decryption to all programs regardless of whether they were previously unprotected in the analog domain. Either tuner can be controlled to tune to a DOCSIS channel or MPEG native transport on QAM.

Performance

BW: 54-1002 MHz, 64-1024 QAM, Noise Figure: <12dB, Channel Selection
Latency: <100 msec

Key Technologies
The basic technologies are the same as used in today's digital set-top box. Cost targets are achieved because of lack of a user interface other than the universal remote control, the use of mature DOCSIS 2.0 signaling, and potential silicon integration for high-volume devices. To provide as much transparency as possible for channel surfing, means should be provided to allow low latency for channel changes.

Hardware Description
- The input of this device is connected to the cable plant with two tuners. Both tuners cover the 54-1002 MHz cable downstream. Either tuner can be used to receive and demodulate DOCSIS transport or to extract native MPEG/ASTC over QAM (up to 1024 QAM is supported).
- The upper signal flow path allows for the MPEG2 transmission stream to flow to a baseband processor implemented with DSP building blocks. The baseband processor demultiplexes the transmission stream and extracts the particular program selected by the subscriber. The program is applied to the conditional access system. The baseband processor is also equipped with a second advanced video codec algorithm that is under the control of the head-end (see Video Codec section).
- The CA system is as described in the conditional access discussion presented herein.
- MPEG packets can also be unicast to the device via the DOCSIS path. These DOCSIS carried packets can be placed into the MPEG convergence sub-layer defined in DOCSIS or can also be encapsulated in a standard IP packet.
- Firmware in the ODA is stored in flash memory and can be updated via the TFTP protocol as in DOCSIS to update general control firmware or the key exchange subsystem of the CA. DOCSIS network management systems can be employed.

External interfaces
These include: Input F-connector to coax plant, Output F-connector to channel 3 or 4 input to consumer device (e.g. TV or VCR), and wireless remote control protocol. AC mains connection required for power. A firmware defined expansion port shall be provided for future use (e.g. USB-2).

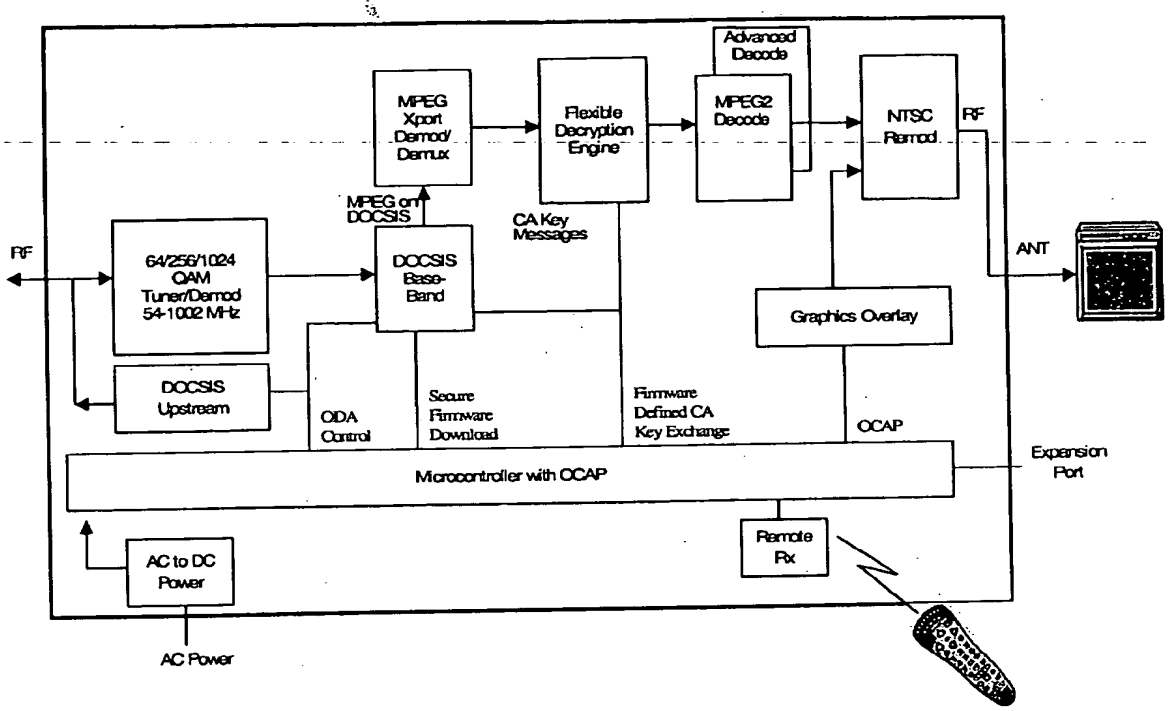
All-DOCSIS 2-Way ODA

Unlike the full function ODA, this device has only a DOCSIS path for management and program content delivery. While this is perhaps the lower cost ODA, it may require offsetting higher costs in the head-end.

Except for a new remote control, the ODA is largely transparent to basic video subscribers. The services remain the same, and the small ODA device is most likely placed behind the TV set.

In addition to allowing more efficient use of cable spectrum, the addressable two-way capability may also assist in promoting self-installation of the ODA devices, because it will enable operators to provide incentives such as free on-demand content and it will provide information to CSRs who may be called upon to help subscribers complete installation tasks.

Figure 11: All-DOCSIS 2-Way ODA Hardware Architecture



Key next generation features of all-DOCSIS 2-way ODA
The reference architecture for the all-DOCSIS ODA supports MPEG video over DOCSIS by either broadcast video encoded in the downstream DOCSIS MPEG convergence sublayer, or alternatively unicast as MPEG over IP.

Functions
Compared to the full function ODA, this ODA uniquely provides the following:

- Single tuner supports access to digital broadcast unencrypted or encrypted services but can apply digital decryption to all programs regardless of whether they were previously unprotected in the analog domain.
- Employs the same DOCSIS 2.0 2-way communications path used for program delivery for signaling back to head-end to facilitate MSO implementations of switched digital video.
- Video programs can be delivered to this device via the DOCSIS path as the MPEG convergence sub-layer in DOCSIS or as MPEG over IP.

Performance
BW: 54-1002 MHz, 64-1024 QAM, Noise Figure: <12dB, Channel Selection
Latency: <100 msec

Key Technologies
The basic technologies are the same as used in today's digital set-top box. Cost targets are achieved because of lack of a user interface other than the universal remote control, use of mature DOCSIS 2.0 signaling, and silicon integration enabled by high volume. Low latency to support channel surfing should be supported.

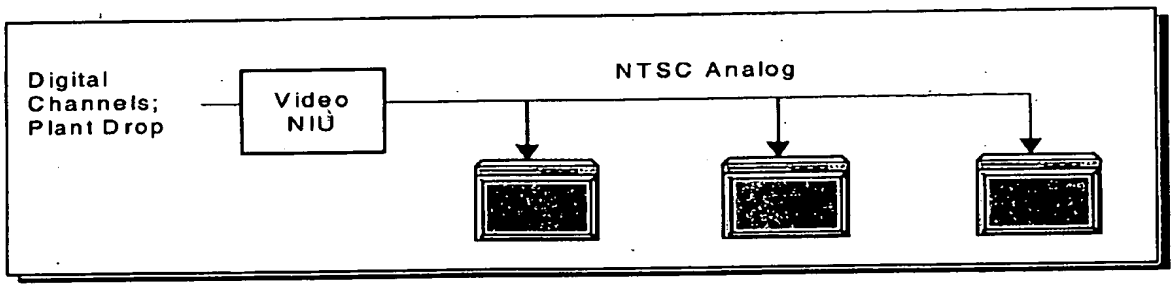
Hardware Description
This input of this device is connected to the cable plant with a DOCSIS tuner covering 54-1002 MHz cable downstream. The tuner is used in the same manner as a standard cable modem to tune to the DOCSIS downstream channel. The video can be placed into the MPEG convergence sublayer defined in DOCSIS or can also be encapsulated in a standard IP packet. The DSP and other firmware in the ODA are stored in flash memory and can be updated via the TFTP protocol defined in the DOCSIS standard.

External interfaces
These include: Input F-connector to coax plant, Output F-connector to channel 3 or 4 input to consumer device (e.g. TV or VCR), and wireless remote control protocol. AC mains connection required for power. A firmware defined expansion port is provided for future use (e.g. USB-2).

Video Network Interface Unit (NIU)

In some subscriber households with numerous analog cable outlets, it may be more economical to provide the ODA functionality through a digital-to-analog block converter at the service entrance. This device would provide whole-house coverage rather than requiring multiple separate ODAs.

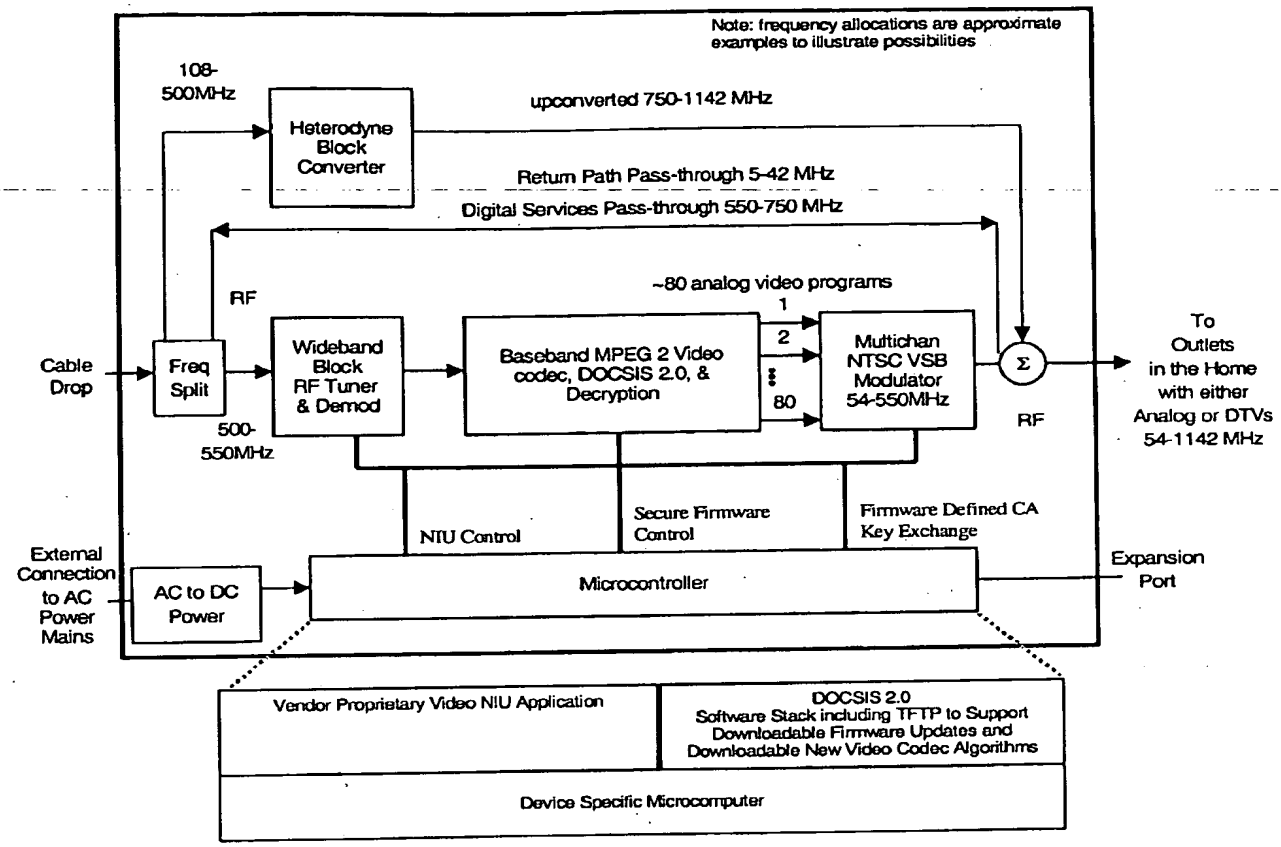
Figure 12: Example of Video NIU deployment



As with the ODA, the Video NIU is intended as a transition device that allows subscribers who have cable-ready analog TVs and other analog devices (e.g. VCRs) to continue to receive their existing services in a manner that is as transparent as possible, while the formerly analog channels are use to carry digitally compressed signals on the cable plant.

Unlike the ODA, the Video NIU performs a block transcoding of digital signals to analog.

Figure 13: Video NIU Hardware Architecture



Key next generation features of Video NIU

- Allows for migration of some (or all) analog channels to compressed digital.
- Provides greater transparency to existing subscribers with no set-top boxes as there is no need to use a special remote control and there would be no latency in channel surfing.
- The band from 54-108 MHz is unassigned so that a future migration to a mid-split system can be accommodated.
- Fully compatible with NGNA CA and DOCSIS signaling employed in other subscriber video CPE.

Function

- This device is a whole house digital video to analog block converter that takes a 48 MHz wideband RF channel modulated with a multiplexed MPEG transport stream containing 80 independent program streams. The device de-multiplexes and decodes the program streams and remodulates the decoded videos into conventional NSTC VSB RF in the band from 54MHz to 550MHz.

- The device is designed to be located at the service entrance so that one or more analog outlets following the device will see what appears to be 80 conventional analog channels.
- The device supports NGNA CA fully compatible with that described for ODAs and other subscriber video devices.
- The device includes embedded DOCSIS for management and control.
- The device preferably supports only a single mode MPEG-2 compatible video codec. In the example shown in the Figure, the device splits the RF band so that 500-550MHz is used for the 80 programs that were formerly analog. The band above 550MHz is passed through to support all digital services in the home, including digital video and HSD. The band from 108-500 MHz is up-converted and added to the in-home RF distribution to allow use of this band for new digital services. The band from 54-108 MHz is left unused so that a long-term future migration to a mid-split system can be accommodated.

Performance
Environmental: indoor mounting 0 to +60 degrees C, dry environment. Compliant with FCC Regulations 47CFR76.

Key Technologies
There are conventional technologies to implement a 48MHz wide RF tuner and the following the tuner the wideband IF output could be converted by one or more highly linear A/D converters. The high-speed digital stream following the A/D converter(s) is/are then applied to a powerful bank of DSP processing that demodulates the 80 multiplexed program streams into 80 separate baseband audio/video programs. The technology required to implement the 80 channel analog NTSC modulator might be implemented using direct digital synthesis or perhaps by using a comb filter based generator of CW carriers modulated using Hilbert Transform based modulators to cancel the lower sideband.

Hardware Description
This device is digital video-to-analog block converter that takes a 48 MHz portion of the spectrum modulated with 80 independent program streams, de-multiplexes the streams, and then re-modulates the 80 channels back into conventional NTSC RF analog channels. The device includes a microcomputer to manage downloadable firmware upgrades. The video codec is fixed single mode MPEG-2. NGNA CA is supported in the baseband processor.

External Interfaces
The device has two F-connectors for input and output and one connection to AC mains power.

Subscriber Video Devices (SVDs)

Subscriber video devices (SVDs) include a range of low- and high-end devices that incorporate next generation network attributes.

This equipment is provided either by the cable operator or, preferably, at retail by consumer electronics suppliers. Some of the SVDs will operate as set-top boxes. Other SVDs could include 2-way cable-ready digital TV sets.

Examples of next generation SVD options described herein include:

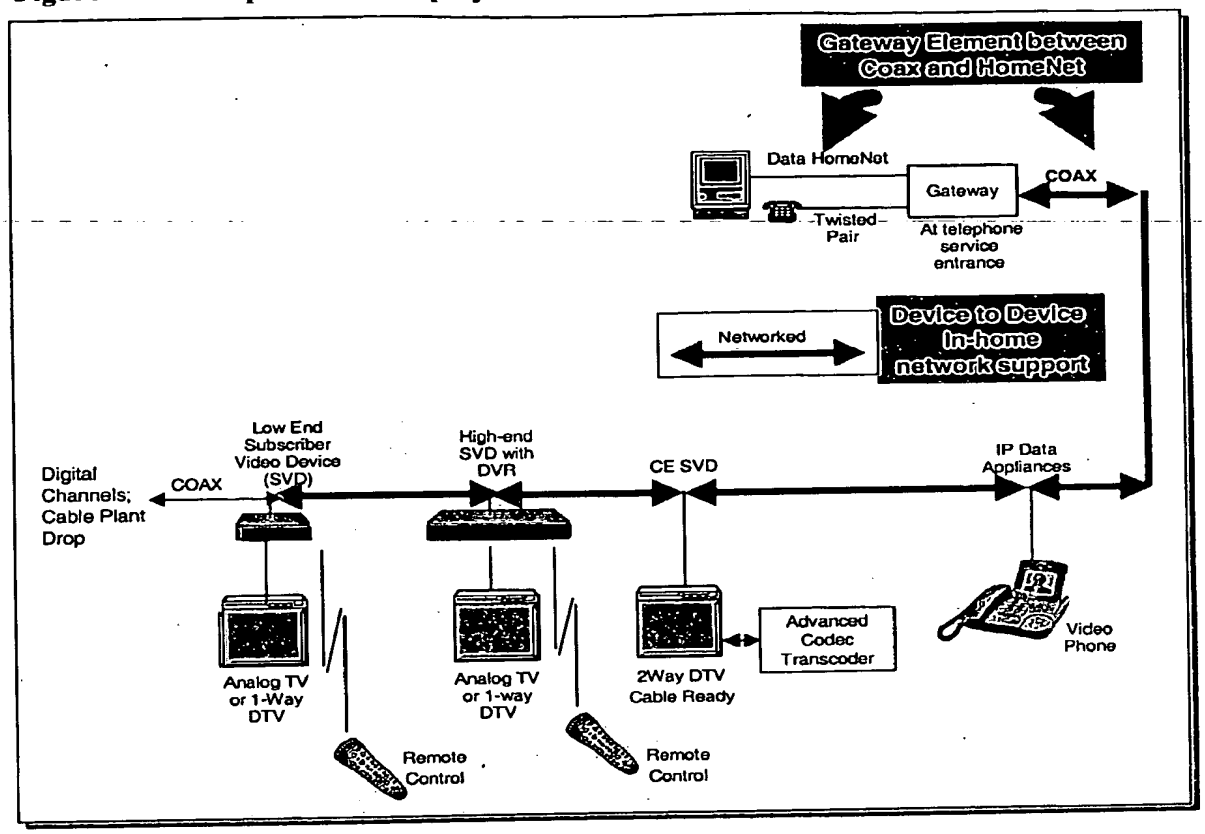
- Low-end SVD
- High-end SVD
- 2-way cable-ready DTV compliant with future MSO/CE agreement

These devices are designated as SVDs because each goes beyond the conventional set-top box functions in that it also supports networking over the in-home network. Each of these devices can access resources in any other device on the network. Thus the lowest order device can deliver the features and capabilities of the highest order device. The reference design of the present invention also supports copy-protected and rights-managed interchange of content between any of the SVDs on the home network.

The low-end and high-end SVDs can be provided by the MSO or purchased at retail while the cable-ready two-way DTV is most likely to be purchased at retail. Details on the cable-ready two-way DTV are included herein to illustrate the NGNA aspects of the reference design and to show how MSO-provided devices would work in a synergistic way with the CE-provided devices.

The following figure illustrates the SVDs' ability to network to other SVDs and to other compatible devices. In this figure, the cable-ready two-way DTV is additionally equipped with an ancillary device, an Advanced Codec Transcoder, which allows cable operators to upgrade the networks to more advanced video compression systems while continuing to support CE devices that are only capable of decoding MPEG2 transport streams.

Figure 14: Example of SVD deployment for subscriber with home data network.



SVDs have as their principle function the delivery of video entertainment. Additional devices may offer video communications and may be networked with SVDs, such as video conferencing devices and other forms of IP appliances.

Each of the SVDs shares certain next generation network features with the ODAs:

- Includes means for decryption of the program content and a conditional access system that is fully compatible with the CA suggested for the ODAs.
- The CA design assumes that the decryption is performed in internal configurable hardware for cost reasons. The high-end SVD is a partial exception in that it also is designed to support a CableCARD but defaults to remotely configured internal CA when the CableCARD is removed.
- The conditional access approach is as described herein.
- 2-way capable in order to support several NGNA objectives:
  - — Reduced operating costs by giving MSO customer service and maintenance staff visibility of the subscriber equipment status.
  - — Enable the customer to access advanced services such as on-demand content.
  - — Allow for implementation of switched digital broadcast should an MSO elect to use this technology to gain additional spectrum.
  - — Improve overall security against theft of service by allowing for downloading new firmware for conditional access and other firmware updates.

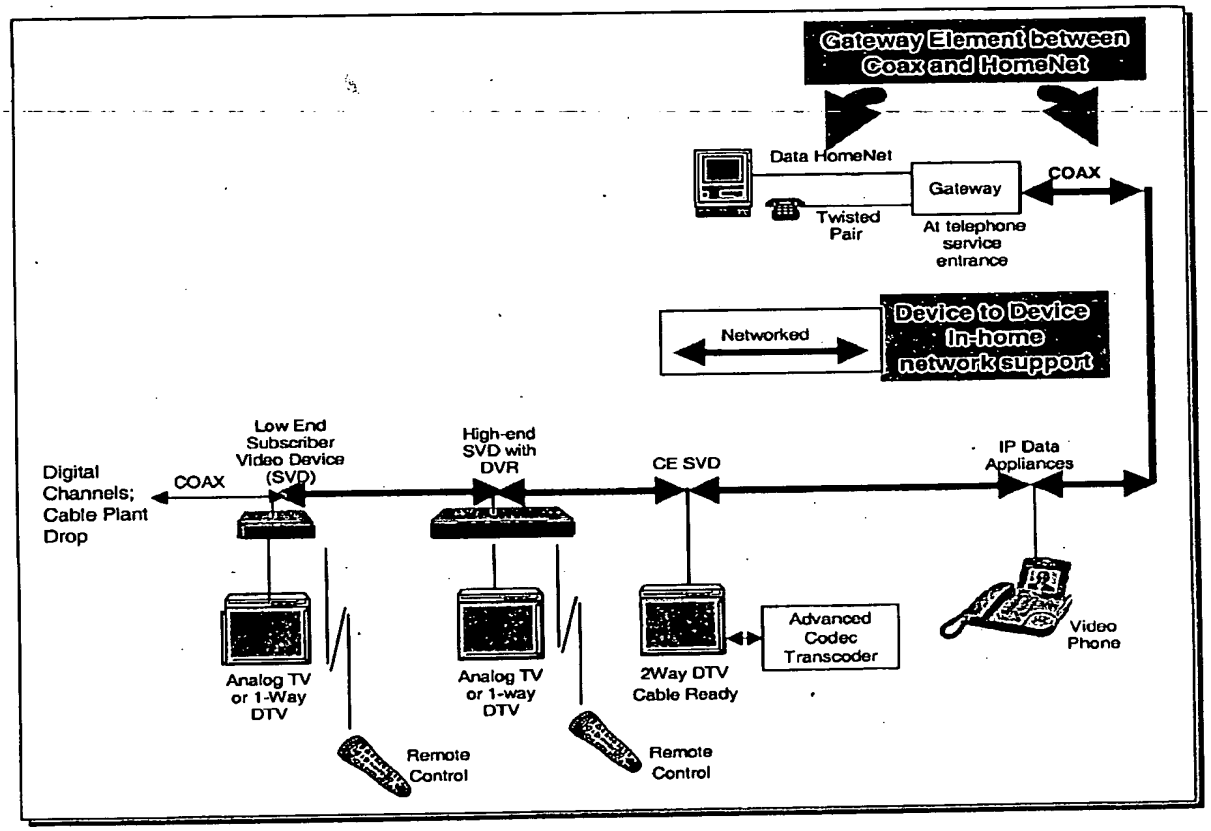
- Uses DOCSIS 2.0 to leverage the manufacturing scale economies of DOCSIS integrated circuits and also to leverage the intrinsic capabilities of DOCSIS 2.0 with BPI+ to provide a 2-way secure authenticated channel between the head end and the device.
- Provided with dual mode video decoders that support existing MPEG-2 ATSC compatible compression and also an advanced video codec to facilitate increasing the video program bandwidth by at least 2X (see Video Codec section).
- Designed to be "retail friendly" so that they provide benefits that a subscriber might well wish to purchase. For example, the high-end SVD might offer DVR or recordable DVD. Furthermore given well-defined interface standards, any mix of MSO provided or subscriber purchased devices can work together.
- Video programs can be delivered to this device as either native MPEG packets modulated on QAM or alternatively via the DOCSIS path as the MPEG convergence sublayer in DOCSIS (as described in the Video Transport section).
- The device can output in either analog or digital interfaces including DVI and 1394 with CE industry standard copy protection.
- An expansion port is provided under the control of the microcontroller firmware.
- Supports SVD-to-SVD in-home networking over the coax network, for example, in the spectrum above 750MHz.
- The in-home network includes encryption and 2-way secure authenticated channels. The purpose of the in-home network over coax is to allow remote access to advanced SVDs, including DVRs or DTVs elsewhere in the home connected to the coax network.

Also contemplated are possible variations on the SVD reference models that are not explicitly described herein and that may have significant cost implications. For example, a low-end SVD may be designed without support for OCAP or native applications. Because all SVDs would include support for home networking, this low-end SVD could work in conjunction with a high(er)-end SVD that does support OCAP applications. This variant of the low-end SVD could be sold at retail if the subscriber were also equipped with a high(er)-end SVD. Examples of SVD variants are summarized in the following chart.

SVD	OCAP	Native Applications	Available at retail
High-end model	Y	All OCAP	Y
Low-end model	Y	All OCAP	Y
Low-end – SVD Variation - No Apps	N	None	Y, with high-end SVD

Low-end Subscriber Video Device

Figure 15. Low-end Subscriber Video Device (SVD) Hardware Architecture



Key next generation features
The low-end SVD is designed for low cost yet can deliver the features of higher-end devices so that subscribers can enjoy enhanced functions at a lower cost than if a high-end device were at every outlet.

This device supports 2-way and on-demand features and other applications that operate through OCAP middleware.

Functions
In addition to the general features of SVDs described earlier, the low-end SVD has dual tuners that can either support video MPEG over QAM or DOCSIS.

Performance
BW: 54-1002 MHz, 64-1024 QAM, Noise Figure: <12dB, Channel Selection
Latency: <100 msec

Key Technologies
The basic technologies are the same as used in today's digital set-top box; however, cost targets are achieved because of CA that allows for multiple sources of supply and greater silicon integration.

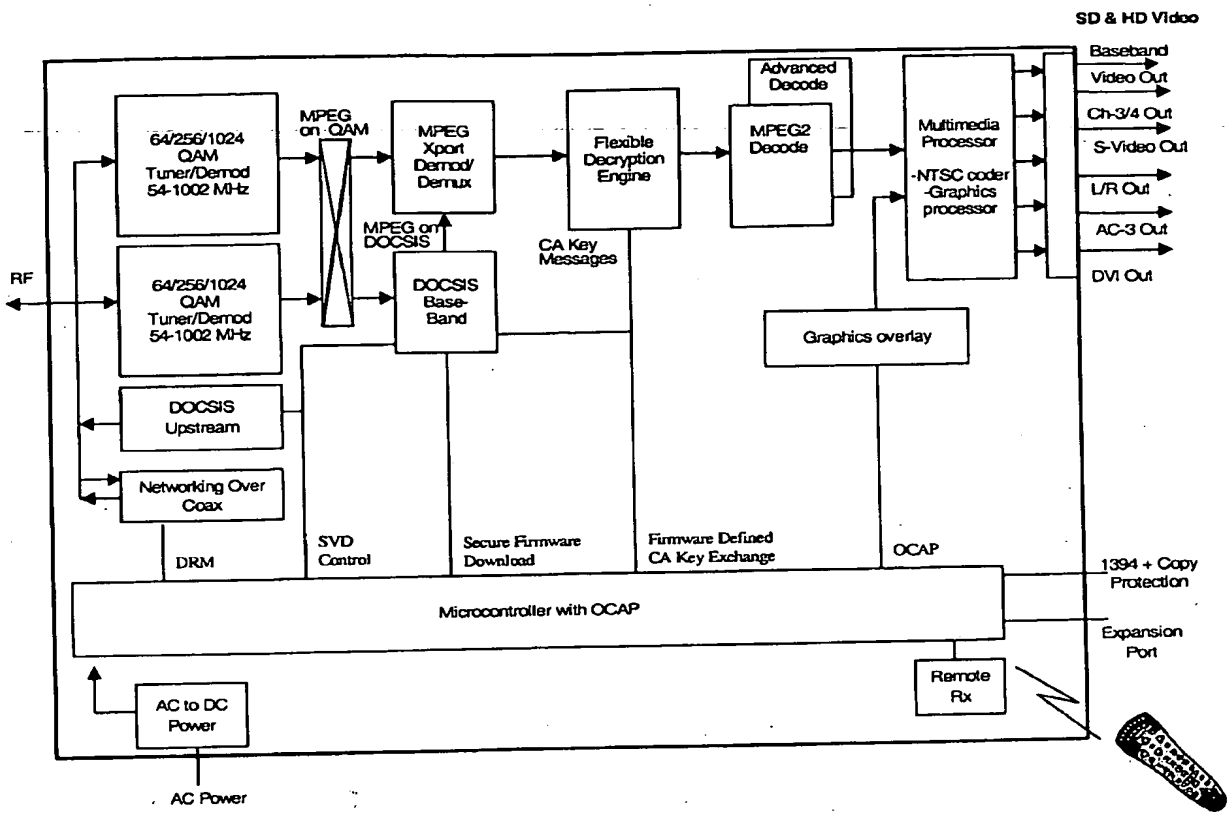
Hardware Description
- This input of this device is connected to the cable plant with two tuners. Both tuners cover the 54-1002 MHz cable downstream and can be used for either video or DOCSIS.
- The upper signal flow path allows for the ATSC MPEG2 transmission stream to flow to an IF/Baseband processor implemented with DSP building blocks. The baseband processor de-multiplexes the transmission stream to extract the particular program selected by the subscriber's remote control. The program is applied to the open standard CA system.
- The baseband processor is also equipped with a second advanced video codec algorithm (e.g. MPEG4/P10 or WIN9) that is under the control of the head-end (see Video Codec section).
- The CA system is as described in the conditional access discussion herein.
- Video transport as described herein in the Video Transport section.
- The DSP and other firmware in the SVD is stored in flash memory and can be updated via the TFTP protocol defined in the DOCSIS standard or via the Common Download specification defined in OpenCable, e.g., to download a new video codec with processing power needs comparable to MPEG4.

External Interfaces
These include: Input F-connector to coax plant, Output F-connector to channel 3 or 4 input to consumer device (e.g. TV or VCR), Baseband NTSC audio and video, DVI and 1394 outputs, and infrared window compliant with IRDA protocol. An expansion port (TBD, possibly USB2) is also provided.

CCCI 0122 PRV

High-end Subscriber Video Device

Figure 16. High-end Subscriber Video Device (SVD) Hardware Architecture



Key next generation features

In addition to features in low-end SVDs, the high-end SVD has the following:

- Supports the functionality of a "Gateway Element" by allowing lower end SVDs to deliver features of higher-end devices so that subscribers can enjoy enhanced functions at a lower cost than if a high-end device were at every outlet.
- Additional tuner that allows for simultaneous watching and independent recording of programs on a DVR or recordable DVD.
- Provides a multi-stream CableCARD interface port so that a CableCARD can be inserted to support legacy CA as required by the CableCARD agreements, compliant with the OpenCable Multistream CableCARD Interface specification. (see http://www.opencable.com/specifications).

Function

In addition to functions in the low-end SVD, the high-end SVD provides:

- Dual tuners for video and 3rd tuner for DOCSIS.
- DVR functions

Performance
BW: 54-1002 MHz, 64-1024 QAM, Noise Figure: <12dB, Channel Selection
Latency: <100 msec

Key Technologies
The basic technologies are the same as used in today's digital set-top box. Cost targets are achieved because the use of CA that allows for multiple sources of supply and greater silicon integration.

Hardware Description
The hardware components of the high-end SVD as the same as in the low-end device, plus the following:

- This input of this device is connected to the cable plant with three video tuners plus a DOCSIS tuner. All tuners cover the 54-1002 MHz cable downstream and can be controlled to demodulate either MPEG over QAM or DOCSIS.

External Interfaces
These include: Input F-connector to coax plant, Output F-connector to channel 3 or 4 output to consumer device (e.g. TV or VCR), Baseband NTSC audio and video, DVI and 1394 outputs, and infrared window compliant with IRDA protocol. An expansion port (TBD, possibly USB-2) is also provided.

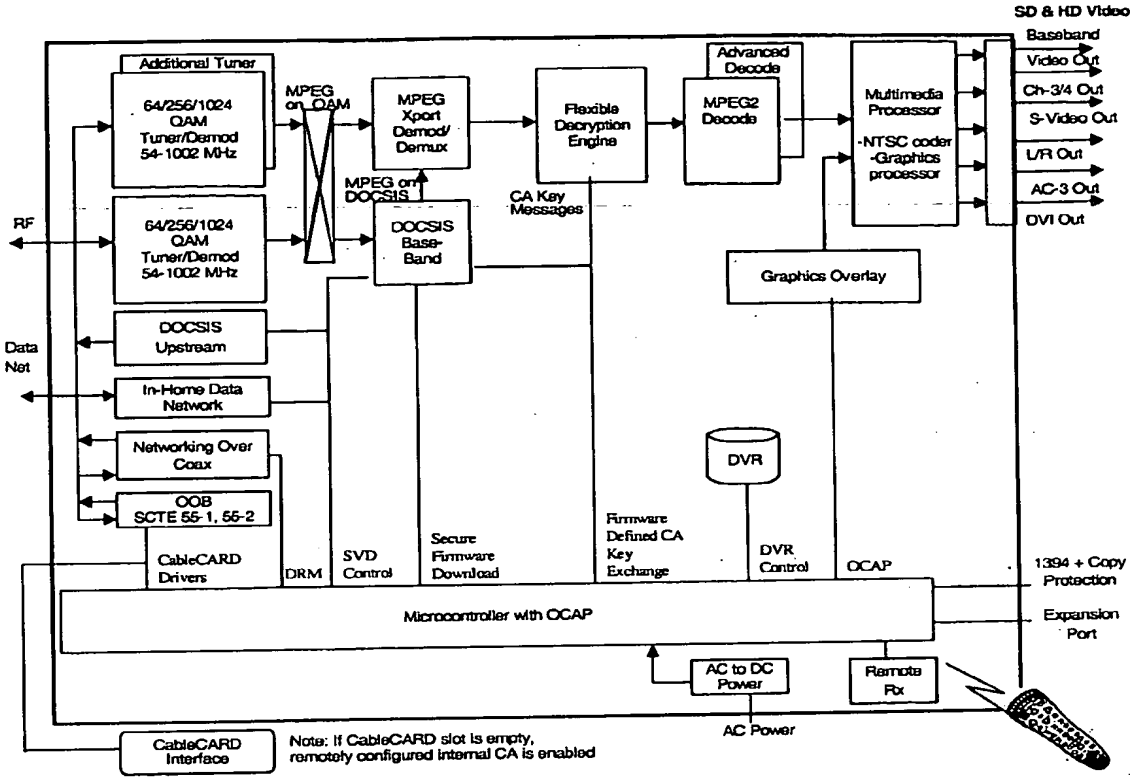
Two-Way Cable-Ready Digital TV

In order to understand the fit between the low-end and high-end SVDs, included herein is a reference design for a 2-way cable-ready digital TV that is compatible with the SVDs and the signals on the cable plant.

This DTV is essentially the same as the high-end SVD with the DVR function removed and a display added. A further difference is that preferably only MPEG-2 support is assumed in the DTV with no support for a dual-mode video codec. As described below, an Advanced Codec Transcoder would allow 2-way cable-ready DTVs to accommodate advanced video codecs in the future.

Because of the commonality between 2-way DTVs and high-end SVDs, further information is not provided other than the following reference design Figures:

Figure 17: Two-way cable-ready DTV hardware architecture



Advanced Codec Transcoder

For subscribers with two-way digital-cable-ready CE video devices capable of receiving only MPEG2 compressed video, Advanced Codec Transcoders (ACT) will enable continued use of their CPE when cable operators upgrade their networks to more advanced compression systems. The most convenient interface for such a device may be at the CableCARD interface port for several reasons:

- In the general case, the remotely configured internal CA will be active and the CableCARD slot will be empty and available.
- The MPEG transport stream is exposed at the CableCARD so that the advanced compressed video program stream can be extracted from the MPEG transport stream for transcoding back to MPEG2.
- The host device is designed to support copy protection on the interface between the CableCARD and the host and the ACT can make use of this copy protection without additional costs.

The Advanced Codec Transcoder is designed for use when it becomes important to upgrade from MPEG2 to an advanced video codec. For example, the Transcoder could accept an MPEG4/part 10 transport stream and transcode it into a MPEG2

transport stream so the legacy CE device with only MPEG2 support will continue to operate normally.

The Advanced Codec Transcoder is provisioned with a dual mode video codec which supports existing MPEG 2 ATSC compatible compression and also a future advanced video codec that facilitates increasing the video program bandwidth by at least 2X. This particular feature of the device is useful with for 2-way DTVs and other digital-cable-ready CE devices should the MSO decide to employ an advanced video codec on the plant.

The choice of MPEG2 or the 2nd advanced codec is under control of the head-end.

Other CPE Devices

Examples of next generation network CPE have been described herein, including options for ODAs and a range of SVDs.

Given the proliferation of new video, data, and multimedia services possibilities, and increasing convergence between these services, it is likely that additional next generation CPE will be developed that will connect directly and indirectly to the cable network.

Device manufacturers are already incorporating multiple functions into cable modems such as various combinations of layer 3 router firewalls, data hubs, voice telephony MTAs, and home networking transport (e.g. WiFi, HPNA, HomePlug, etc), and are likely also to integrate some of the next generation network functions into future cable modems and other subscriber devices. Examples of next generation network functions that are candidates for creative integration into CPE include in-home networking within and between the guaranteed and authorized service domains, and CableHome functions that allow management and visibility of subscriber devices from the head-end. Examples of new subscriber devices include:

Multifunction gateway. The core of this device is currently available, including a cable modem, layer 3 router firewall, and a voice telephony MTA. A next generation version of this device adds CableHome capabilities of visibility and management of devices from the head-end. It also includes a bridging feature allowing interaction between SVDs compatible with the in-home network protocols and devices on the in-home data network. Such a device supports applications such as:

- Allowing PCs with a suitable bridge to use the coax network as a means to access high-speed data services.
- Allowing consumer-owned PCs or servers on the in-home data or coax network to communicate displayable messages or control messages to SVDs.
- Enabling the telephony MTA to send caller ID messages (or other messages) to SVDs.
- Allowing SVDs to access billing or service information regarding subscribers' interactive multimedia/data services.

As with all next generation network CPE devices, this next generation gateway device should be CableHome compliant to facilitate remote management and customer support.

CPE Monitor. The CPE Monitor is a transitional device that implements the CableHome functionality of head-end remote visibility and management of devices on the private side of a non-CableHome customer-installed layer 3 router firewall. This device would not be necessary if the subscriber's firewall were CableHome-compliant. However, given the large installed base of customer-owned, non-CableHome-compliant, home networks, this device provides benefits of CableHome compliance while preserving subscribers' investments in existing home networks. The CPE Monitor is connected to the private side of the subscriber's firewall somewhere on the in-home network. It is enabled to create a secure tunnel through the subscriber's firewall so that head-end systems have access to traffic and devices on the subscriber's system. By having visibility of the traffic intensity and device status, the head-end could provide some measure of QoS or admission control for traffic that is required to transit the private in-home network. By having access to management protocols (e.g. SNMP), the head-end could have visibility of the status and health of subscriber devices on the private side of the network.

Outside Plant Network Segment

Cable operators are rapidly adding new services and capabilities while migrating from largely analog to digitally-coded downstream signals. Substantial growth in bandwidth-intensive HD programs is anticipated. Various forms of on-demand services are being introduced and, depending on how they are implemented, they could result in either more or less consumption of downstream bandwidth resources. In the upstream direction, applications are developing such as telecommuting, peer-to-peer file exchange, and multiplayer gaming that will require more symmetrical upstream bandwidth allocations.

While accommodating the new applications, the outside plant needs to continue to support legacy investments in subscriber and head-end equipment. For example, the need to support legacy digital set-top boxes with proprietary CA during the time period while MSOs may choose to transition to a new proprietary or non-proprietary CA suggests a potential need to partly simulcast program content in both legacy as well as the new CA.

Goals of the NGNA with respect to the outside plant include:

- Provide non-limiting bandwidth for the introduction of new services
- Leverage past investments in the HFC plant with new investments made on a "success basis" in which each investment can be amortized in short timeframe tied to specific new revenue opportunities

Key next generation features of outside plant architecture include:

- Leveraging the existing HFC investments by not requiring increasing bandwidth above 750MHz and also not requiring splitting fiber nodes below 500 homes passed.

- Maintaining the plant in good condition so that future migration to 1024 QAM and an advanced video codec can be supported
- Reserving spectrum between 54MHz and 108MHz so that a future migration to a mid split plant can be accommodated (accordingly, NGNA devices will have increased agility range in the upstream transmitters for future potential use).

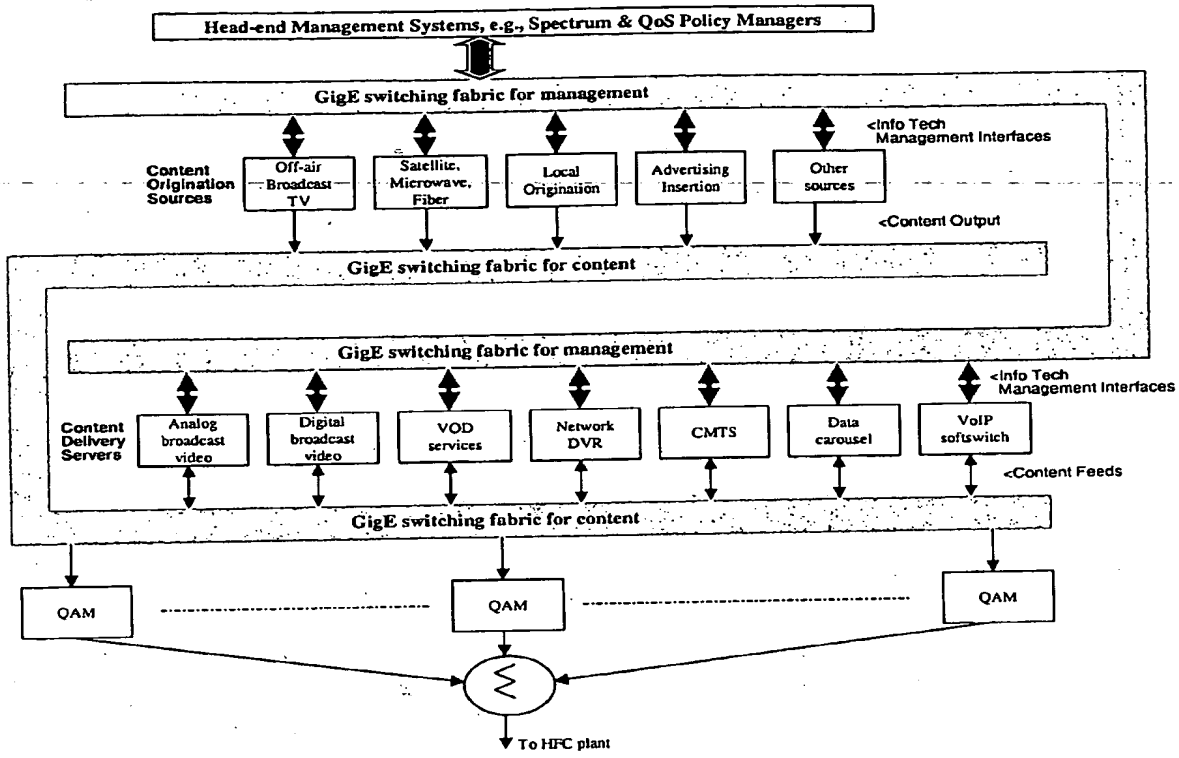
Head-end Network Segment

The NGNA is an *integrated multimedia architecture*. Integration represents a significant departure from cable systems' traditional independent "stovepipes" for video, data, and telephony. Benefits of integration include:

- More efficient use of system resources (e.g. spectrum allocations, QAM streams);
- Facilitating inter-working of network elements supplied by multiple vendors to enable more open competition, to extend the service life of the installed base, to provide flexibility for new service introductions, and to provide scalability to accommodate a range of system sizes;
- Providing a platform for innovation and rapid service creation that involves cross-over access among the former service stovepipes (e.g., viewing movies on a PC or caller ID on a TV).

To support these objectives, a head-end architecture that will support on-demand video, flexible CA, 2-way multimedia messaging, and integration between data, messaging, and entertainment. The following Figure describes a head-end server architecture.

Figure 18: Head-end server architecture



Key next generation features of head-end server architecture include:

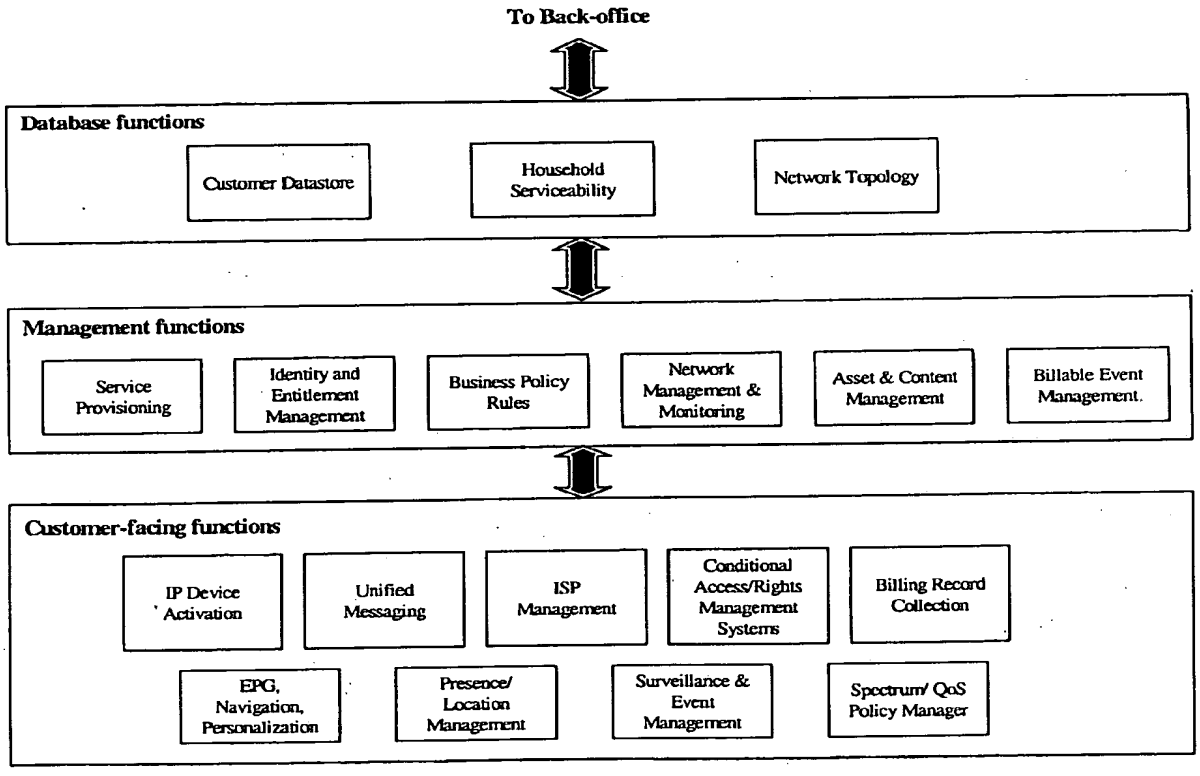
- Applications are managed across all services by a QoS Policy Manager task and a Spectrum/QAM Resource Manager. The QoS Policy Manager has capability to operate autonomously in the event of communications failure with back office systems.
- The control and RF aspects of the head-end servers are separate so that common third party resource management and network operations applications can manage the head-end as an integrated system rather than as standalone service specific subsystems.
  - *QAM modulators*: Separate the modulators from head-end servers such as VOD servers and CMTS so that each server has a GigE compatible data interface.
  - *GigE switching fabric for content*: Add GigE switches under control of a system resource manager so any server can have data switched to any QAM stream and any content source can switch content to any server.
  - *System resource managers*: Add new spectrum and QoS policy resource manager servers that are aware of traffic loads, QoS needs, subscriber entitlements, and have policies and algorithms to dynamically assign spectrum and QAM stream resources in the most efficient matter.

- *GigE switching fabric for management*: Provide a standard management plane interface by means of a GigE switching fabric so that each service can be managed and controlled by external IT management systems via open APIs.

DSM-CC (Digital Storage Media – Command and Control) and DSG (DOCSIS Set-top Gateway) are used for control and management of video based services.

To support the management and control of the head-end servers and content sources, the following Figure shows a reference architecture for the management and information technology components.

Figure 19: Head-end Management Architecture



As shown in the Figure, the head-end management architecture includes customer-facing functions, management functions, and database functions.

As an example of a *customer-facing function*, ISP Management provides for email, personal web pages (PWP), and portals; it supports management of subscribers' ISP accounts, cross-selling of services via the web pages, and interfaces for communities and subscriber interactions for games or other activities.

Examples of *management functions* include:

- Service Provisioning for subscribers via internal systems and via external third-party systems, e.g., to support local number portability and/or complementary services.
- Business Policy Rules that set priorities for different kinds of traffic and for different relationships with third-parties, and that support marketing and bundling initiatives. These rules may derive not only from cable operators but also from their content or service providers.
- Billable Events that rate transactions and calculate charges to subscribers or partners such as advertisers.

A major component of this reference design refers to interfaces between the head-end information technology (IT) infrastructure and back office systems by means of shared (or replicated) databases between the head-end and back-office IT systems. Examples of *database functions* include:

- Customer Datastore maintains customer identities, and stores information on the services and CPE associated with specific customers.
- Household Serviceability maintains information on availability of services and capabilities associated with locations, such as high-speed data, telephony, or high-definition TV. Such information may be made available to retailers, perhaps through Go2Broadband, to support retail distribution channels for cable equipment and services.
- Network Topology maintains information on network attributes such as strand maps, fiber counts to fiber nodes, GigE network facilities, multiplexers and/or dedicated fibers to business customers, and wireless network extensions via strand-mounted WiFi access points.

IT platforms can arguably be designated as either head-end or back office systems. A preferred rule to make this designation is that the head-end IT platforms are any real-time systems that must be online to support subscriber service delivery. Non-real-time platforms that are used for functions such as network management, billing, configuration management, provisioning, and customer support are assumed to be in the back office. Given this rule, the interfaces to the back office are largely relegated to the non-realtime provisioning of the head-end, monitoring, data collection, policy management, and other management functions.

Glossary

1394	IEEE 1394, also called Firewire
AC-3	Audio coding standard developed by Dolby Labs
AES	Advanced Encryption Standard
API	Application Programming Interface
ASD	Authorized Service Domain
ATSC	Advanced Television Study Committee
AVC	Advanced Video Coding
BPI+	DOCSIS Baseline Privacy Plus
CA	Conditional Access
CAS	Conditional Access System
CAT	Conditional Access Table
CBC	Cipher Block Chaining
CBR	Constant bit rate
CCI	Copy Control Information
CE	Consumer electronics
CMTS	Cable modem termination system
Codec	Coder/Decoder
CORBA	Common Object Request Broker Architecture
CPE	Customer premises equipment
CSA	Common Scrambling Algorithm
CW	Control Word
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Services Architecture for Network Traffic
DOCSIS	Data Over Cable Service Interface Specification
DRM	Digital Rights Management
DSCP	DiffServe Code Point
DSG	DOCSIS Set-top Gateway
DSM-CC	ISO/IEC Digital Storage Media – Command and Control
DSP	Digital signal processing
DSS	Digital Signature Standard
DTV	Digital TV
DVB	Digital Video Broadcast
DVI	Digital Video Interface
DVR	Digital video recording
ECB	Electronic Code Book
ECM	Entitlement Control Message
ECPA	Electronic Communication Privacy Act
EMC	Electromagnetic compatibility
EMM	Entitlement Management Message
EPG	Electronic program guide
FIPS	Federal Information Processing standard
FPGA	Field Programmable Gate Array
GigE	Gigabit Ethernet
GSD	Guaranteed Service Domain
HDTV	High definition TV
HFC	Hybrid fiber coax
HPNA	Home Phoneline Networking Alliance

HSD	High speed data
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPDR	IP Data Record
J2EE	Java Two Enterprise Edition
KEK	Key Encryption Keys
Layer 2	Link layer in Open Systems Interconnection (OSI) framework
Layer 3	Network layer in OSI stack; Layer in firewall in which routing is based on IP-address.
LDAP	Lightweight Directory Access Protocol
LEC	Local exchange carrier
Low-Split	Common HFC frequency assignment in which upstream (to head-end) is below 42 MHz and downstream (to customer) is above 54MHz.
L/R	Left/Right baseband audio outputs from stereo system
MAC	Media Access Control
MIB	Management Information Base
Mid-split	Upstream/downstream cross-over point at ~100MHz to increase available upstream bandwidth.
MoCA	Multimedia Over Coax Alliance
MPEG	Motion Picture Experts Group
MPTS	Multiple Program Transport Streams
MTA	Multimedia Terminal Adapter
NAT	Network address translation
NCAS	NGNA conditional access system
nDVR	Network DVR
NE	Network elements
NGNA	Next Generation Network Architecture
NIU	Network Interface Unit
OCAP	OpenCable Applications Platform
ODA	Outlet Digital Adapter
OEM	Original equipment manufacturer
ODRL	Open Digital Rights Language Initiative
OOB	Out of band
OSS	Operations Support System
PC	Personal Computer
PES	Program Elementary Stream
PHY	Physical layer
PID	Packet Identifier
PMA	Performance Monitoring Application
PS	Portal services
PSI	Program Specific Information
QAM	Quadrature Amplitude Modulation
QoS	Quality of service
QPSK	Quadrature phase shift keying
RAN	Regional area network
RMS	Rights Management System
ROSI	Return on security investment
RSA	Public key cryptosystem developed by Rivest, Shamir, Adleman; also company by same name marketing public key technology.
RSVP	Internet protocol to reserve resources for streaming content QoS.

RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SCTE	Society of Cable Television Engineers
SD	Secure Digital
SHA-1	Secure hash standard #1
SIP	Session Initiation Protocol
SNMP	Simple network management protocol
SOC	System on a chip
SPTS	Single Program Transport Streams
SVD	Subscriber video device
S-Video	High quality video interface, derived from Super VHS signal format
TFTP	Trivial File Transfer Protocol (Trivial FTP)
TOS	Type of Service (also DiffServ Code Point, DSCP)
TCP	Transmission Control Protocol
TS	Transport stream
UDCP	Unidirectional Digital Cable Product
UDP	User Datagram Protocol
UI	User interface
UPnP	Universal Plug and Play
USB	Universal serial bus
VBR	Variable bit rate
VLAN	Virtual Local Area Network
VSB	Vestigial SideBand
VOD	Video on demand
VoIP	Voice over IP
XML	Extensible Markup Language
XrML	Extensible Rights Markup Language